

378.744  
BO  
AM 1933  
sp

**Boston University  
College of Liberal Arts  
Library**

THE GIFT OF The Author

378.744

BO

AM. 1933

SP

p7587

BOSTON UNIVERSITY

GRADUATE SCHOOL

Thesis

DOMAINS AND REDUCIBILITY

(An elementary introduction to the Galois Theory)

by

Joseph Spear

(A.B., Harvard University, 1913)

submitted in partial fulfilment of the

requirements for the degree of

Master of Arts

1933

BOSTON UNIVERSITY  
COLLEGE OF LIBERAL ARTS  
LIBRARY

P 7587

378.744  
B0  
AM 1933  
sp

## OUTLINE AND PAGE INDEX

|                                                            | Page |
|------------------------------------------------------------|------|
| Introduction on the Solution of the Algebraic Equation . . | 1    |
| History of Galois . . . . .                                | 2    |
| Purpose of this Paper . . . . .                            | 5    |
| Domain of Rationality . . . . .                            | 6    |
| A Divisor of a Domain . . . . .                            | 7    |
| The Domain of Rational Numbers . . . . .                   | 7    |
| The Process of Adjoining . . . . .                         | 7    |
| Domains: Zero, Integers, Fractions . . . . .               | 8    |
| Reducibility in a Domain . . . . .                         | 8    |
| Algebraic and Transcendental Domains . . . . .             | 10   |
| Euclid's Algorithm . . . . .                               | 10   |
| Theorem on Roots of Two Equations . . . . .                | 10   |
| Gauss's Lemma . . . . .                                    | 11   |
| Gauss's Lemma Applied to the Cubic . . . . .               | 13   |
| Gauss's Lemma Applied to the Quartic . . . . .             | 13   |
| Gauss's Lemma Applied to the Quintic . . . . .             | 15   |
| A Test for Irreducibility . . . . .                        | 17   |
| Definition of a Cyclotomic Equation . . . . .              | 19   |
| The Cyclotomic Equation is Irreducible . . . . .           | 20   |
| Multiple Roots . . . . .                                   | 20   |
| Degree. Conjugate. Normal . . . . .                        | 21   |
| Conjugate, Primitive, Imprimitive Numbers . . . . .        | 23   |
| Primitive and Imprimitive Domains . . . . .                | 24   |
| Theorem on Symmetric Functions of Roots . . . . .          | 24   |

# OUTLINE AND PAGE INDEX

|      |                                                                  |
|------|------------------------------------------------------------------|
| Page |                                                                  |
| 1    | Introduction on the Solution of the Algebraic Equation . . . . . |
| 2    | History of Galois . . . . .                                      |
| 3    | Purpose of this Paper . . . . .                                  |
| 4    | Domain of Rationality . . . . .                                  |
| 5    | A Divisor of a Domain . . . . .                                  |
| 6    | The Domain of Rational Numbers . . . . .                         |
| 7    | The Process of Adjoining . . . . .                               |
| 8    | Domain: Zero, Integer, Fraction . . . . .                        |
| 9    | Reducibility in a Domain . . . . .                               |
| 10   | Algebraic and Transcendental Domains . . . . .                   |
| 10   | Galois's Algebra . . . . .                                       |
| 10   | Theorem on Roots . . . . .                                       |
| 11   | General . . . . .                                                |
| 12   | Gauss's Lemma Applied to the Cubic . . . . .                     |
| 13   | Gauss's Lemma Applied to the Quartic . . . . .                   |
| 13   | Gauss's Lemma Applied to the Quintic . . . . .                   |
| 14   | A Test for Irreducibility . . . . .                              |
| 15   | Definition of a Cyclotomic Equation . . . . .                    |
| 16   | The Cyclotomic Equation is Irreducible . . . . .                 |
| 17   | And the Roots . . . . .                                          |
| 18   | Degree, Conjugate, Normal . . . . .                              |
| 19   | Conjugate, Primitive, Irrational Numbers . . . . .               |
| 20   | Primitive and Irrational Numbers . . . . .                       |
| 21   | Theorem on Synthetic Functions of Roots . . . . .                |

Digitized by the Internet Archive

in 2016 with funding from

Boston Library Consortium Member Libraries

|                                                                               | Page |
|-------------------------------------------------------------------------------|------|
| Theorem on Numbers as Roots of Equations . . . . .                            | 24   |
| Evaluation of an Indeterminate Fraction . . . . .                             | 29   |
| Theorem on the Function of any Primitive Number . . . . .                     | 30   |
| Theorem on Conjugate Numbers as Roots of an Irreducible<br>Equation . . . . . | 32   |
| Normal Equations . . . . .                                                    | 34   |
| Theorem on Primitive Numbers as Roots of Normal Equations                     | 34   |
| The Galois Domain . . . . .                                                   | 36   |
| Conclusion . . . . .                                                          | 39   |
| Bibliography . . . . .                                                        | 41   |

|    |       |                                                           |
|----|-------|-----------------------------------------------------------|
| 24 | ..... | Theorem on Numbers as Roots of Equations                  |
| 29 | ..... | Definition of an Indeterminate Equation                   |
| 30 | ..... | Theorem on the Function of any Primitive Number           |
|    |       | Theorem on Composite Numbers as Roots of an Irreducible   |
| 32 | ..... | Equation                                                  |
| 34 | ..... | Normal Equations                                          |
| 34 | ..... | Theorem on Primitive Numbers as Roots of Normal Equations |
| 36 | ..... | The Galois Domain                                         |
| 39 | ..... | Conclusion                                                |
| 41 | ..... | Bibliography                                              |

## INTRODUCTION ON THE SOLUTION OF THE ALGEBRAIC EQUATION.

The question as to whether all algebraic equations were solvable by the use of radicals had received much attention and it had long been believed that all algebraic equations could be solved by the use of radicals. Although no proof had been presented, even as late as the latter part of the eighteenth century leading mathematicians believed this to be true. In 1799, an Italian physician, Paolo Ruffini, printed a proof of the insolvability by radicals of the general algebraic equations of degree above the fourth. This, however, was not a rigorous proof, and it was not until 1826 that such a rigorous proof was established, by N. H. Abel. He showed that the general equation above the fourth degree could not be so solved. Evariste Galois made great advances in the general theory in this field, and in particular in adapting it to the work in groups. Galois showed that algebraic equations and groups of substitutions could be so made to correspond that the character of the equation could be brought out clearly. Thus it is by means of groups associated with the particular equation that one can determine whether or not the equation is solvable by radicals.

This paper intends only to give an introduction to the work of Galois, presenting in elementary form and in detail all the steps necessary for the establishment of the so-called Galois Domain.

INTRODUCTION ON THE SOLUTION OF THE ALGEBRAIC EQUATION

The question as to whether all algebraic equations were solvable by the use of radicals had received much attention and it had long been believed that all algebraic equations could be solved by the use of radicals. Although no proof had been presented, even as late as the latter part of the eighteenth century leading mathematicians believed this to be true. In 1799, an Italian physician, Paolo Ruffini, published a proof of the impossibility of radicals of the general algebraic equations of degree above the fourth. This, however, was not a rigorous proof, and it was not until 1802 that such a rigorous proof was established, by L. N. Abel. He showed that the general equation above the fourth degree could not be solved. Ever since Abel's made great advances in the general theory in this field, and in particular in adapting it to the work in groups. Abel's showed that algebraic equations and groups of substitutions would be as much to correspond that the character of the solutions would be known, one clearly. This it is by means of groups associated with the polynomial equation that one can determine whether or not the equation is solvable by radicals.

This paper intends only to give an introduction to the work of Galois, presenting in elementary form and in detail all the steps necessary for the establishment of the so-called Galois' Theorem.

## HISTORY OF GALOIS.

Evariste Galois was born October 25, 1811, in a small town near Paris. His father and paternal grandfather were proprietors of a school, his maternal grandfather was an eminent jurist, and his mother was well educated in the classics. Thus, Galois had an excellent inheritance from both sides of his family. His mother was Galois' only teacher until Evariste reached the age of twelve. He then started attending school. At fifteen he became absorbed in the study of mathematics. He showed at once a remarkable mind in the field of mathematics, and was fascinated by the works of such men as Legendre and others. At seventeen he made his first discoveries in the field of the theory of equations, which he presented to Cauchy at the Academy of Sciences. This paper was never heard of again. At about the same time, 1829, he published his first paper.

Desiring at this time to enter Ecole Polytechnique, the leading mathematics school in France, he presented himself twice for examination and failed both times. There are probably two reasons for these failures. Galois worked exclusively with broad aspects of the subjects, and many things seemed trivial and self-evident to him so he did not bother explaining details. His discussions at the examinations, therefore, sounded obscure and unsatisfactory. These examinations were held before large audiences and Galois was greatly embarrassed standing at the blackboard before these people. The other reason

HISTORY OF CALIFORNIA

Everette Gelais was born October 22, 1911, in a small town near Iowa. His father and paternal grandfather were proprietors of a school, his maternal grandfather was an eminent jurist, and his mother was well educated in the classics. Thus, Gelais had an excellent inheritance from both sides of his family. His mother was Gelais' only teacher until Everette reached the age of twelve. He then started attending school. At fifteen he became absorbed in the study of mathematics. He showed at once a remarkable mind in the field of mathematics, and was fascinated by the works of such men as Lagrange and others. At seventeen he made his first discovery in the field of the theory of equations, which he presented to Congress at the Academy of Sciences. This paper was never heard of again. At about the same time, 1929, he published his first paper.

Desiring at this time to enter Ecole Polytechnique, the leading mathematical school in France, he presented himself twice for examination and failed both times. There are probably two reasons for these failures. Gelais worked exclusively with broad aspects of the subjects, and many things seemed trivial and self-evident to him so he did not bother explaining them. His discussions at the examinations, therefore, sounded obscure and unsatisfactory. These examinations were held before large audiences and Gelais was greatly embarrassed standing at the blackboard before these people. The other reason

now given for his failure is that it is believed that the examiners were incapable of appreciating the explanations of this genius. His failures greatly disappointed him. He went to Ecole Preparatoire, a more elementary school. About this time his father, who was mixed up in revolutionary politics, committed suicide.

At eighteen Galois published four memoires, one of which was a brief summary of some results regarding algebraic solution of equations, and another on the theory of numbers, now called Galois' imaginaries, and very important in the theory of groups. In January, 1830, he placed great hope in another memoire concerning important researches, which he worked out in detail. He presented this to Fourier, who died shortly afterwards, and this paper was also never heard from.

Galois, now, in 1830, entered heart and soul into the revolution against Charles X. The school he was attending objected to his political affiliations, and so he was expelled from the school in December, 1830. At this time, Poisson and others became interested in Galois. Poisson told Galois to rewrite his researches and he would present them to the Academy. Galois, with much hope and enthusiasm, wrote out in great detail the only finished memoire we have of his theory of solutions of equations. The title of this paper translated is "On the Conditions on the Solvability of Equations by Radicals". Galois put so much faith into this promise of Poisson that he opened a school on higher algebra in the back of a bookstore.

now given for his failure is that it is believed that the exam-  
iners were incapable of appreciating the significance of this  
solution. His failure greatly disappointed him. He went to  
Karlo's preparatory school, a more elementary school. About this time  
his father, who was mixed up in revolutionary politics, com-  
mitted suicide.

At sixteen Galois published four memoirs, one of  
which was a brief summary of some results regarding algebraic  
solution of equations, and another on the theory of numbers,  
now called Galois' theorems, and very important in the the-  
ory of groups. In January, 1830, he placed great hope in an-  
other memoir concerning important theorems, which he worked  
out in detail. He presented this to Fourier, who died shortly  
afterwards, and this paper was also never heard from.

Galois, now, in 1830, entered heart and soul into the  
revolution against Charles X. The school he was attending op-  
posed to his political affiliations, and so he was expelled  
from the school in December, 1830. At this time, Fourier and  
others became interested in Galois. Fourier told Galois to  
rewrite his researches and he would present them to the Academy.  
Galois, with much hope and enthusiasm, wrote out in great de-  
tail the only finished memoir we have of his theory of solu-  
tions of equations. The title of this paper translated is  
"On the Conditions on the Solvability of Equations by Radicals".  
Galois put so much faith into this promise of Fourier that he  
opened a school on higher algebra in the back of a bookstore.

All of Galois' great hopes, however, were short-lived because the memoir given to Poisson was returned as unintelligible.

So disappointed was Galois in this that he now went deeper than ever into politics with the reactionary factions of the republican party. He was twice arrested for political offenses, and spent most of the last year and a half of his life in prison. On being finally released, he fought a duel in an affair of love. This resulted in his death, May 31, 1832.

The night before the duel he spent in writing up his mathematical discoveries in the form of a letter to a school friend, Auguste Chevalier. In the letter, he asked Chevalier to beg publicly both Gauss and Jacobi to give their opinion, not on the truth, but on the importance of his theories.

Professor James Pierpont says this is considered one of the most touching documents in the history of science. Here is a young man, about to die, conscious of the importance of his discoveries, spending his last night on earth trying to write up his discoveries to save them for posterity, in spite of the fact that his contemporaries would not accept them.

The letter was not published until the issue in September, 1832, of the Revue Encyclopedique. The Revue also stated that shortly afterwards all of Galois' manuscripts would be published. This did not happen. In 1846, fourteen years later, Liouville edited in his Journal de Mathematiques a part of Galois' work on the solvability of equations by radicals. Here, Liouville stated that on close study he now realized the

All of Calais' great hopes, however, were short-lived because the resolve given to Calais was returned as unattainable. So disappointed was Calais in this that he now went deeper than ever into politics with the revolutionary factions of the republican party. He was twice arrested for political offenses, and spent most of the last year and a half of his life in prison. On being finally released, he fought a duel in an affair of love. This resulted in his death, May 31, 1832.

The night before the duel he spent in writing up his mathematical discoveries in the form of a letter to a school friend, Auguste Chevalier. In the letter, he asked Chevalier to put publicly both names and talent to give their opinion, not on the result, but on the importance of his theories.

Professor James Pierpont says this is considered one of the most important documents in the history of statistics. It is a young man, about to die, considering on the importance of his discoveries, spending his last night on earth trying to write up his discoveries to save them for posterity, in spite of the fact that his contemporaries would not accept them.

The letter was not published until the issue in September, 1833, of the *Revue Mathématique*. The review also stated that shortly afterwards all of Calais' manuscripts would be published. This did not happen. In 1846, fourteen years later, Chevalier edited in his *Journal de Mathématiques* a part of Calais' work on the solvability of equations by radicals. Here, Chevalier stated that on some body he now retained the

entire correctness of Galois' proof of the theorem that "In order that an irreducible equation of prime degree be soluble by radicals, it is necessary and sufficient that all its roots be rational in any two of them."

Liouville hoped to publish all of Galois' writings, but intended probably first to clear up those parts that were vague. Only two papers, however, were published by Liouville, the one which Poisson returned as unintelligible, and part of another. Apparently, Liouville had difficulty in establishing the rigor of some of Galois' work.

In 1852, the theory of Galois on the solvability of equations was for the first time published with complete rigorous proof, in such a way that the ordinary student could understand it.

Kronecker became acquainted with the theory in 1853. Dedekind lectured on it in 1857. The first account of the theory in a text book was in 1866, in Serret's Algebra. Jordan published his treatise on it in 1870. In 1897, the works of Galois were published by La Societe' Mathématique de France with an introduction by Picard. J. Tannery published other writings of Galois in the Bulletin des Sciences Mathématiques in 1906-1907.

#### PURPOSE OF THIS PAPER.

We can thus see that the subject has only been brought to definite conclusions in recent years. The investigation as to whether or not every algebraic equation can be solved by the

entire correctness of Galois' proof of the theorem that "in order that an irreducible equation of prime degree be soluble by radicals, it is necessary and sufficient that all its roots be rational in any two of them."

Lionville hoped to publish all of Galois' writings, but intended probably first to clear up those parts that were vague. Only two papers, however, were published by Lionville, the one which Tisserand returned as unintelligible, and part of another. Apparently, Lionville had difficulty in establishing the rigor of some of Galois' work.

In 1882, the theory of Galois on the solvability of equations was for the first time published with complete rigor and proof, in such a way that the ordinary student could understand it.

Frobenius became acquainted with the theory in 1882. Heberich lectured on it in 1887. The first account of the theory in a text book was in 1883, in Herstein's Algebra. Jordan published his treatise on it in 1870. In 1897, the works of Galois were published by La Courbe, *Mathématiques de France* with an introduction by Poincaré. A. Tannery published other articles of Galois in the *Revue des Sciences Mathématiques* in 1895-1907.

#### IMPORTANCE OF THIS PAPER.

We now turn to the subject that has only been brought to definite conclusions in recent years. The investigation as to whether or not every algebraic equation can be solved by the

use of radicals, as in Cardan's solution of the cubic, or Ferrarri's solution of the quartic, was followed through by men like Lagrange, Gauss, Cauchy, Abel, and Galois. The answer is definitely "no", that the general equation of the fifth degree and above can not ordinarily be solved by radicals and the proof is best obtained by means of groups of substitutions or permutation of letters. Incidentally, the study of groups in this connection also leads to the answer whether every angle can be trisected with ruler and compass, and, also, answers the question as to what regular polygons can be constructed by elementary geometry. The subject is, therefore, entirely too extensive to be covered in a paper of this sort. We shall merely prepare an introduction which will enable one to go further into the subject and shall afford references for such further study.

\* \* \* \* \*

#### DOMAIN OF RATIONALITY.

Given a set of constants or variables, and all the quantities derived from them by a finite number of operations of the four fundamental processes of arithmetic, namely, addition, subtraction, multiplication, division, (division by zero excluded), then the resulting system of quantities is called a Domain of Rationality,  $R$ , or simply a Domain. As an example, all rational numbers form a Domain, because from 1 may be derived all integers by addition and subtraction, and from these all fractions by division.

use of radicals, as in Cardan's solution of the cubic, or  
 Ferrari's solution of the quartic, was followed through by  
 men like Lagrange, Gauss, Cauchy, Abel, and Galois. The an-  
 swer is definitely "no", that the general equation of the fifth  
 degree and above can not ordinarily be solved by radicals and  
 the proof is best obtained by means of groups of substitutions  
 or permutation of letters. Incidentally, the study of groups  
 in this connection also leads to the answer whether every angle  
 can be trisected with ruler and compass, and, also, answers the  
 question as to what regular polygons can be constructed by ele-  
 mentary geometry. The subject is, therefore, entirely too ex-  
 tensive to be covered in a paper of this sort. We shall merely  
 propose an introduction which will enable one to go further  
 into the subject and shall afford references for each further  
 study.

\* \* \* \*

## DOMAIN OF RATIONALITY.

Given a set of constants or variables, and all the  
 quantities derived from them by a finite number of operations  
 of the four fundamental processes of arithmetic, namely, addi-  
 tion, subtraction, multiplication, division, (division by zero  
 excluded), then the resulting system of quantities is called a  
 Domain of Rationality,  $R$ , or simply a Domain. As an example,  
 all rational numbers form a Domain, because from 1 and 0 we de-  
 rived all integers by addition and subtraction, and from these  
 all fractions by division.

### A DIVISOR OF A DOMAIN.

If we are given two domains,  $R$  and  $R'$ , and if all the numbers of domain  $R$  are contained in the domain  $R'$ , then  $R$  is called a divisor of  $R'$ , and  $R'$  is called a domain over  $R$ . Thus the domain consisting of all numbers of form  $a+bi$ , where  $a$  and  $b$  are rational numbers and  $i^2 = -1$  is a domain over the domain of rational numbers, and the domain of rational numbers is a divisor of this domain consisting of all numbers of form  $a+bi$ .

### THE DOMAIN OF RATIONAL NUMBERS.

Let  $R_{(1)}$  represent the domain of rational numbers, i.e. it is the group of numbers made up of all numbers which can be obtained by addition, subtraction, multiplication, and division of the integers, positive and negative, division by zero excluded. Then, obviously,  $R_{(1)}$  is a domain which is a divisor of every domain,  $R_{(i)}$ , because if ' $a$ ' is an element of the domain  $R_i$  then  $\frac{a}{a} = 1$  is an element of the domain  $R_i$ , and from 1 can be derived all the integers by the four arithmetic processes, so all elements of  $R_{(1)}$  can be obtained.

### THE PROCESS OF ADJOINING.

If with all the elements of the domain  $R_{(1)}$ , the element being all rational numbers, we also include the element  $i = \sqrt{-1}$ , then we get a new domain, called  $R_{(1,i)}$ , which consists of all elements of type  $a+bi$ , where  $a$  and  $b$  are rational numbers. This process of obtaining the domain  $R_{(1,i)}$  from domain  $R_{(1)}$  is called adjunction. In general, if to the elements of domain  $R$  we add " $a$ ", which is not already an element of  $R$ ,

## A DIVISION OF A DOMAIN.

If we are given two domains,  $R$  and  $R'$ , and if all the members of domain  $R$  are contained in the domain  $R'$ , then  $R$  is called a divisor of  $R'$ , and  $R'$  is called a domain over  $R$ . Thus the domain consisting of all members of form  $a+bi$ , where  $a$  and  $b$  are rational numbers and  $i^2 = -1$  is a domain over the domain of rational numbers, and the domain of rational numbers is a divisor of this domain consisting of all members of form  $a+bi$ . THE DOMAIN OF RATIONAL NUMBERS.

Let  $R(I)$  represent the domain of rational numbers, i.e. it is the group of numbers made up of all numbers which can be obtained by addition, subtraction, multiplication, and division of the integers, positive and negative, divided by zero excluded. Then, obviously,  $R(I)$  is a domain which is a divisor of every domain,  $R(I)$ , because if  $a$  is an element of the domain  $R$ , then  $\frac{a}{2} = 1$  is an element of the domain  $R(I)$ , and from  $1$  can be derived all the integers by the four arithmetic processes, so all elements of  $R(I)$  can be obtained.

## THE PROCESS OF ADJOINING.

If  $R(I)$  is the domain of the domain  $R(I)$ , the elements of  $R(I)$  are rational numbers, we also include the element  $\sqrt{2}$ , then we get a new domain, called  $R(I, \sqrt{2})$ , which contains all elements of type  $a+b\sqrt{2}$ , where  $a$  and  $b$  are rational numbers. This process of obtaining the domain  $R(I, \sqrt{2})$  from the domain  $R(I)$  is called adjoining. In general, if to the elements of domain  $R$  we add " $a$ ", which is not already an element of  $R$ ,

and also add to R all numbers obtained by the four arithmetic processes on "a" and the elements of R, then this total set of elements form a new domain, called  $R(a)$ , obtained by adjunction of "a" to domain R.

DOMAINS: ZERO, INTEGERS, FRACTIONS.

Obviously, the number zero satisfies the definition of a domain, but it is in itself useless, because all elements of the domain are zero. Also, the integers themselves do not form a domain because division may give fractions. Also, the rational proper fractions themselves would not constitute a domain because addition might give integers, which are new elements not already included in the original group.

REDUCIBILITY IN A DOMAIN.

If  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  is an integral function, where all the coefficients  $a_0, a_1, a_2, \dots, a_{n-1}, a_n$  belong to a domain R, then  $f(x)$  is called a function in the domain R and  $f(x) = 0$  is an equation in the domain R. If  $n=1$  then the function, of the first degree, cannot be factored except for some possible constant factor. If  $n > 1$ , then it may be possible to factor  $f(x)$  where the factors are functions of  $x$  of the lower degree than  $f(x)$  itself. If all these factors have coefficients all of which are members of the domain R, then  $f(x)$  is said to be reducible in the domain R. If all the coefficients of these factors are not all members of the domain R then  $f(x)$  is irreducible in R. In this case, however, where  $f(x)$  is irreducible in R it is possible by

and also add to  $R$  all numbers obtained by the four arithmetic processes on "a" and the elements of  $R$ , then this total set of elements form a new domain, called  $\mathcal{A}(R)$ , obtained by adjunction of "a" to domain  $R$ .

# DOMAINS: ZERO, ENTIRE, FRACTIONS.

Obviously, the number zero satisfies the definition of a domain, but it is in itself useless, because all elements of the domain are zero. Also, the integers themselves do not form a domain because division may give fractions. Also, the rational proper fractions themselves would not constitute a domain because addition might give integers, which are new elements not already included in the original group.

## REDUCIBILITY IN A DOMAIN.

If  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  is an

integral function, where all the coefficients

$a_0, a_1, a_2, \dots, a_{n-1}, a_n$  belong to a domain  $R$ , then  $f(x)$  is

called a function in the domain  $R$  and  $f(x) = 0$  is an equation

in the domain  $R$ . If not then the function, of the first degree,

cannot be factored except for some possible constant factor.

If not, then it may be possible to factor  $f(x)$  where the fac-

tors are functions of  $x$  of the lower degree than  $f(x)$  itself.

If all these factors have coefficients all of which are members

of the domain  $R$ , then  $f(x)$  is said to be reducible in the do-

main  $R$ . If all the coefficients of these factors are not all

members of the domain  $R$  then  $f(x)$  is irreducible in  $R$ . In this

case, however, where  $f(x)$  is irreducible in  $R$  it is possible by

the adjunction of proper elements to find a domain in which  $f(x)$  is reducible.

The function  $f(x) = x^2 + 3x + 2$  is a function in domain of rational numbers  $R_{(1)}$  and is reducible in that domain as it can be factored into  $(x+2)(x+1)$  whose coefficients are all rational numbers. On the other hand  $f(x) = x^2 + 3x - 2$  is in domain  $R_{(1)}$  and is irreducible in  $R_{(1)}$ . But if we factor as follows:  $f(x) = x^2 + 3x - 2 = (x + \frac{3}{2} - \frac{\sqrt{17}}{2})(x + \frac{3}{2} + \frac{\sqrt{17}}{2})$  we see that by adjunction of  $\sqrt{17}$  to  $R_{(1)}$  we get the domain  $R_{(1, \sqrt{17})}$  in which  $f(x) = x^2 + 3x - 2$  is reducible.

Again further examples:

$$f_1(x) = x^2 + 2x + 1 = (x+1)(x+1)$$

$$f_2(x) = x^4 + x^2 + 1 = (x^2 - x+1)(x^2 + x+1)$$

$$f_3(x) = x^2 + x - 1 = (x + \frac{1}{2} - \frac{\sqrt{5}}{2})(x + \frac{1}{2} + \frac{\sqrt{5}}{2})$$

$$f_4(x) = x^2 + x + 1 = (x + \frac{1}{2} - \frac{\sqrt{3}}{2}i)(x + \frac{1}{2} + \frac{\sqrt{3}}{2}i)$$

$$f_5(x) = x^2 + 1 = (x+i)(x-i)$$

Here  $f_1(x)$  and  $f_2(x)$  are reducible in  $R_{(1)}$  but the other functions are not reducible in  $R_{(1)}$ .  $f_3(x)$  is reducible in  $R_{(1, \sqrt{5})}$ , while  $f_4(x)$  is reducible in  $R_{(1, \sqrt{3}i)}$ .  $f_5(x)$  is reducible in  $R_{(1, i)}$ . All the functions above are reducible in  $R_{(1, i, \sqrt{5}, \sqrt{3})}$ , and this is the smallest domain in which they are reducible.

Similarly whether the equation  $f(x) = 0$  is reducible or irreducible in domain  $R$  depends on whether the function  $f(x)$  itself is reducible or not in the domain  $R$ .

the adjunction of proper elements to find a domain in which  $f(x)$  is reducible.

The function  $f(x) = x^2 + 3x + 2$  is a function in domain of rational numbers  $R_1$  and is reducible in that domain as it can be factored into  $(x+2)(x+1)$  whose coefficients are all rational numbers. On the other hand  $f(x) = x^2 + 3x + 2$  is in domain  $R_1$  and is irreducible in  $R_1$ . But if we factor as follows:  $f(x) = x^2 + 3x + 2 = (x + \frac{3 - \sqrt{17}}{2})(x + \frac{3 + \sqrt{17}}{2})$  we see that by adjunction of  $\sqrt{17}$  to  $R_1$  we get the domain  $R_2$  in which  $f(x) = x^2 + 3x + 2$  is reducible.

Again further examples:

$$f_1(x) = x^2 + 3x + 1 = (x+1)(x+1)$$

$$f_2(x) = x^2 + x + 1 = (x - \frac{1}{2} + \frac{\sqrt{3}}{2}i)(x - \frac{1}{2} - \frac{\sqrt{3}}{2}i)$$

$$f_3(x) = x^2 + x - 1 = (x + \frac{1}{2} + \frac{\sqrt{5}}{2}i)(x + \frac{1}{2} - \frac{\sqrt{5}}{2}i)$$

$$f_4(x) = x^2 + x - 1 = (x + \frac{1}{2} + \frac{\sqrt{5}}{2}i)(x + \frac{1}{2} - \frac{\sqrt{5}}{2}i)$$

$$f_5(x) = x^2 + 1 = (x-i)(x+i)$$

Here  $f_1(x)$  and  $f_5(x)$  are reducible in  $R_1$  but the other functions are not reducible in  $R_1$ .  $f_2(x)$  is reducible in  $R_2$ , while  $f_3(x)$  is reducible in  $R_3$ .  $f_4(x)$  is reducible in  $R_4$ . All the functions above are reducible in  $R_5$ , and this is the smallest domain in which they are reducible.

Similarly whether the equation  $f(x) = 0$  is reducible or irreducible in domain  $R$  depends on whether the function  $f(x)$  itself is reducible or not in the domain  $R$ .

## ALGEBRAIC AND TRANSCENDENTAL DOMAINS.

If to our rational number domain  $R(1)$  we adjoin an algebraic number, that is, we adjoin a number which is a root of the algebraic equation of form

$f(x) \equiv a_0x^n + a_1x^{n-1} + \dots + a_n = 0$ , where all the "a" coefficients are integers, then the new domain is called an algebraic domain. If to  $R(1)$  we adjoin a transcendental number, as  $e$  or  $\pi$ , we get a new domain called a transcendental domain.

## EUCLID'S ALGORITHM.

The common factor of any two rational polynomials in  $x$  can be obtained by Euclid's algorithm, which includes only the four fundamental processes of arithmetic. Therefore, if the two polynomials are both in the domain  $R$ , not only will the common factor be in  $R$ , but all the elements in the coefficients throughout the entire algorithm will be in the domain  $R$ .

## THEOREM ON ROOTS OF TWO EQUATIONS.

It is often desirable to learn whether certain functions are reducible in our rational number domain  $R(1)$ , without actually finding the factors of these functions. Towards this we establish the following theorem:

If  $f(x) = 0$  and  $F(x) = 0$  are two equations in the domain  $R$ , and if  $f(x) = 0$  has a root which satisfies  $F(x) = 0$ , and if  $f(x)$  is irreducible in domain  $R$ , then all the roots of  $f(x) = 0$  satisfy  $F(x) = 0$ .

Proof:  $f(x)$  and  $F(x)$  must have a common factor because by hypothesis their equations have a common root. This

# ALGEBRAIC AND TRANSCENDENTAL DOMAINS

If to our rational number domain  $R_1$  we adjoin an algebraic number, that is, we adjoin a number which is a root of the algebraic equation of form

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = 0, \text{ where all the "a" coefficients are integers, then the new domain is called an algebraic domain. If to } R_1 \text{ we adjoin a transcendental number, as e or } \pi, \text{ we get a new domain called a transcendental domain.}$$

## EUCLID'S ALGORITHM

The common factor of any two rational polynomials in  $x$  can be obtained by Euclid's algorithm, which involves only the four fundamental processes of arithmetic. Therefore, if the two polynomials are both in the domain  $R$ , not only will the common factor be in  $R$ , but all the elements in the coefficients throughout the entire algorithm will be in the domain  $R$ .

## THEOREM ON ROOTS OF TWO EQUATIONS

It is often desirable to learn whether certain functions are reducible in our rational number domain  $R_1$ , without actually finding the factors of these functions. Towards this

we establish the following theorem:

If  $f(x) = 0$  and  $g(x) = 0$  are two equations in the domain  $R$ , and if  $f(x) = 0$  has a root which satisfies  $g(x) = 0$ , and if  $g(x)$  is irreducible in domain  $R$ , then all the roots of

$$f(x) = 0 \text{ satisfy } g(x) = 0.$$

Proof:  $f(x)$  and  $g(x)$  must have a common factor because by hypothesis their equations have a common root. This

common factor is obtainable by Euclid's algorithm. But  $f(x)$  is irreducible in the domain  $R$ , therefore it has no factors in domain  $R$  except itself or a possible constant factor, and Euclid's algorithm introduces no elements except those of the domain of  $f(x)$ . Therefore, the common factor of  $f(x)$  and  $F(x)$  must be either  $f(x)$  itself or  $f(x)$  multiplied by a constant. So  $f(x)$  is a factor of  $F(x)$  and so all roots of  $f(x) = 0$  are roots of  $F(x) = 0$ . So if  $f(x)$  is irreducible in  $R$  and if  $F(x)$  is in  $R$  and if  $f(x)$  is not itself a factor of  $F(x)$ , then  $f(x)$  and  $F(x)$  can not have any common factor in  $R$ , except a possible constant. Because if  $f(x)$  and  $F(x)$  did have such a common factor in  $R$  then  $f(x)$  would be reducible in  $R$ , which is contrary to the hypothesis, or  $f(x)$  and  $F(x)$  would have a common factor not in  $R$ , which would mean that Euclid's algorithm would introduce elements into the coefficients of the algorithm which are not in  $R$ , and this is impossible.

#### GAUSS'S LEMMA.

If a polynomial  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  has integral coefficients and can be factored into two polynomials with rational coefficients, then the coefficients of the two polynomials will be integral coefficients.

Proof: Assume the factors of  $f(x)$  are  $G(x)$  and  $H(x)$ , i.e.  $f(x) = G(x).H(x)$  where  $G$  and  $H$  are rational. If  $G(x)$  has fractional coefficients reduce all to the least common denominator. Do same in  $H(x)$ . So we can write

common factor is obtainable by Euclid's algorithm. But  $f(x)$  is irreducible in the domain  $R$ , therefore it has no factors in  $R$  except itself or a possible constant factor, and Euclid's algorithm introduces no elements except those of the domain of  $f(x)$ . Therefore, the common factor of  $f(x)$  and  $g(x)$  must be either  $f(x)$  itself or  $f(x)$  multiplied by a constant. So  $f(x)$  is a factor of  $g(x)$  and so all roots of  $f(x) = 0$  are roots of  $g(x) = 0$ . So if  $f(x)$  is irreducible in  $R$  and if  $f(x)$  is in  $R$  and if  $f(x)$  is not itself a factor of  $g(x)$ , then  $f(x)$  and  $g(x)$  can not have any common factor in  $R$ , except a possible constant. Because if  $f(x)$  and  $g(x)$  did have such a common factor in  $R$  then  $f(x)$  would be reducible in  $R$ , which is contrary to the hypothesis, or  $f(x)$  and  $g(x)$  would have a common factor not in  $R$ , which would mean that Euclid's algorithm would introduce elements into the coefficients of the algorithm which are not in  $R$ , and this is impossible.

GAUSS'S LEMMA.

If a polynomial  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$  has integral coefficients and can be factored into two polynomials with rational coefficients, then the coefficients of the two polynomials will be integral coefficients.

Theory: Assume the factors of  $f(x)$  are  $g(x)$  and  $h(x)$ , i.e.,  $f(x) = g(x) \cdot h(x)$  where  $g$  and  $h$  are rational. If  $g(x)$  has fractional coefficients reduce all to the least common denominator. Do same in  $h(x)$ . So we can write

$$G(x) = \frac{b_0 + b_1x + b_2x^2 + \dots}{m} \quad H(x) = \frac{c_0 + c_1x + c_2x^2 + \dots}{n}$$

Let K be the highest common factor of  $b_0, b_1, b_2, \dots$ , therefore K and m are relatively prime, because since m is the least common multiple of  $b_0, b_1, b_2, \dots$  these b's and m can have no common factor.

So we can write  $G(x) = \frac{K \cdot g(x)}{m}$  where the coefficients of  $g(x)$  have no common factor.

Similarly let L be the highest common factor of  $c_0, c_1, c_2, \dots$  and so L and n are relatively prime and we can write  $H(x) = \frac{L \cdot h(x)}{n}$  where the coefficients in  $h(x)$  have no common factor. So  $f(x) = G(x) \cdot H(x) = \frac{K \cdot g(x)}{m} \cdot \frac{L \cdot h(x)}{n}$ . Since by hypothesis  $f(x)$  has integral coefficients, therefore  $\frac{KL}{mn}$  must be an integer. Since K and m are relatively prime, therefore L is divisible by m, so  $L = pm$ , where p is an integer. Similarly since L and n are relatively prime, therefore K is divisible by n and so  $K = qn$  where q is an integer.

Therefore, substituting we have

$$f(x) = G(x) \cdot H(x) = \frac{qn \cdot g(x)}{m} \cdot \frac{pm \cdot h(x)}{n} \quad \text{where all the coefficients} \\ = p \cdot q \cdot g(x) \cdot h(x)$$

are integers.

Now if we are given a polynomial with integral coefficients, as  $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$  we can assume that  $a_0 = 1$ , without any loss in the generality of our work, because if  $a_0$  does not equal 1 we can by substitution of a new variable  $y = a_0x$  obtain the function with unity as the



coefficient of the term of highest degree. Therefore, let  $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$  where all the  $a$ 's are integers. If  $x=\alpha$  makes  $f(\alpha) = 0$  then  $x-\alpha$  is a factor of  $f(x)$  and by Gauss's Lemma  $\alpha$  is an integer and must be a factor of  $a_n$ . We have here, therefore, a test for the reducibility of certain functions. If  $n=2$ ,  $f(x)$  is a quadratic polynomial in domain  $R(1)$ , and the condition that it be reducible in  $R(1)$  is that its  $a_n$  have an integral factor  $\alpha$  such that  $f(\alpha) = 0$ .

#### GAUSS'S LEMMA APPLIED TO THE CUBIC.

If  $n=3$  then  $f(x)$  in  $R(1)$  to be reducible in  $R(1)$  must have at least one linear factor,  $(x-\alpha)$  in  $R(1)$  such that  $f(\alpha) = 0$  and  $\alpha$  must be a factor of  $a_n$ .

#### GAUSS'S LEMMA APPLIED TO THE QUARTIC.

If  $n=4$ , there are two possibilities in testing for reducibility. If it has a linear rational factor then proceed as in  $n=3$ . If it has no linear rational factor then it has no cubic rational factor. So we need test only for quadratic rational factors, of form  $x^2 + b_1x + b_2$ . We proceed to divide  $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$  by  $x^2 + b_1x + b_2$  and determine the condition that there be no remainder, where  $b_1$  and  $b_2$  are integers which we are to find.

coefficient of  $x^m$  is not zero. Therefore, let  
$$f(x) = x^m + a_1 x^{m-1} + \dots + a_m$$
  
be the polynomial. If  $x-a$  is a factor of  $f(x)$ ,  
and by Gauss's lemma  $a$  is an integer and must be a factor of  
 $a_m$ . We have here, therefore, a test for the reducibility of  
certain functions. If  $a_1, f(x)$  is a rational polynomial in  
domain  $\mathbb{Z}_p$ , and the condition that it be reducible in  $\mathbb{Z}_p$  is  
that there must be an integral factor  $g(x)$  such that  $f(x) = g(x) \cdot h(x)$ .  
GAUSS'S LEMMA APPLIED TO THE CUBIC.

If  $n=3$ , then  $f(x)$  in  $\mathbb{Z}_p$  to be reducible in  $\mathbb{Z}_p$  must  
have at least one linear factor,  $(x-a)$  in  $\mathbb{Z}_p$ , such that  
 $f(a) = 0$  and  $a$  must be a factor of  $a_m$ .  
GAUSS'S LEMMA APPLIED TO THE QUARTIC.

If  $n=4$ , there are two possibilities in testing for  
reducibility. If it has a linear rational factor then proceed  
as in  $n=3$ . If it has no linear rational factor then it has no  
rational factor. We need tests only for quadratic factors.  
Let  $f(x)$  be of form  $x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$ . We proceed to divide  
 $f(x)$  by  $x^2 + px + q$  and get  $f(x) = (x^2 + px + q)(x^2 + rx + s) +$   
where the condition that there be no remainder, where  $p, q, r, s$   
are integers which we are to find.

$$\begin{array}{r}
 x^2 + (a_1 - b_1)x + (a_2 - b_2 - a_1b_1 + b_1^2) \\
 x^2 + b_1x + b_2 \overline{) x^4 + a_1x^3 + a_2x^2 + a_3x + a_4} \\
 \underline{x^4 + b_1x^3 + b_2x^2} \\
 (a_1 - b_1)x^3 + (a_2 - b_2)x^2 + a_3x + a_4 \\
 \underline{(a_1 - b_1)x^3 + (a_1b_1 - b_1^2)x^2 + (a_1b_2 - b_1b_2)x} \\
 (a_2 - b_2 - a_1b_1 + b_1^2)x^2 + (a_3 - a_1b_2 + b_1b_2)x + a_4 \\
 \underline{(a_2 - b_2 - a_1b_1 + b_1^2)x^2 + b_1(a_2 - b_2 - a_1b_1 + b_1^2)x + b_2(a_2 - b_2 - a_1b_1 + b_1^2)} \\
 [(a_3 - a_1b_2 + b_1b_2) - b_1(a_2 - b_2 - a_1b_1 + b_1^2)]x + a_4 - b_2(a_2 - b_2 - a_1b_1 + b_1^2)
 \end{array}$$

In order to have no remainder

$$(1) \quad (a_3 - a_1b_2 + b_1b_2) - b_1(a_2 - b_2 - a_1b_1 + b_1^2) = 0$$

$$(2) \quad a_4 - b_2(a_2 - b_2 - a_1b_1 + b_1^2) = 0$$

From (2) we get  $a_2 - b_2 - a_1b_1 + b_1^2 = \frac{a_4}{b_2}$

We substitute this in equation (1) and get

$$(a_3 - a_1b_2 + b_1b_2) - b_1\left(\frac{a_4}{b_2}\right) = 0 \quad \text{or}$$

$$a_3b_2 - a_1b_2^2 + b_1b_2^2 - b_1a_4 = 0$$

Solving for  $b_1$  we get (3)  $b_1 = \frac{a_3b_2 - a_1b_2^2}{a_4 - b_2^2}$

Now  $b_2$  must be a factor of  $a_4$ . Therefore, try the factors of  $a_4$  as the values of  $b_2$  in equation (3) and see if we get  $b_1$  as an integer. If it does come out an integer, then we have two integral values,  $b_1$  and  $b_2$ , and if this pair of values satisfies (2) then we have the values desired for  $b_1$  and  $b_2$ , and we have  $x^2 + b_1x + b_2$  as a rational factor of

$$\frac{(a_1 - b_1)x^2 + (a_2 - b_2)x + a_4}{(a_1 - b_1)x^2 + (a_2 - b_2)x + a_4} = \frac{(a_1 - b_1)x^2 + (a_2 - b_2)x + a_4}{(a_1 - b_1)x^2 + (a_2 - b_2)x + a_4}$$

In order to have no remainder

$$(1) \quad (a_1 - b_1)x^2 + (a_2 - b_2)x + a_4 = 0$$

$$(2) \quad a_1 - b_1 = 0$$

$$\text{From (2) we get } a_1 - b_1 = 0$$

we substitute this in equation (1) and get

$$(a_2 - b_2)x + a_4 = 0 \text{ or}$$

$$a_2 - b_2 = 0$$

$$\text{Solving for } b_1 \text{ we get (2) } b_1 = \frac{a_1 - b_1}{a_1 - b_1}$$

Now  $b_1$  must be a factor of  $a_1$ . Therefore, try the factors of  $a_1$  as the values of  $b_1$  in equation (2) and see if we get  $b_2$  as an integer. If it does come out an integer, then we have two integral values,  $b_1$  and  $b_2$ , and if this pair of values satisfies (2) then we have the values desired for  $b_1$  and  $b_2$ , and we have  $x^2 + b_1x + b_2$  as a rational factor of

$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$  and  $f(x)$  is reducible in  $R(1)$ .

GAUSS'S LEMMA APPLIED TO THE QUINTIC.

If  $n = 5$  then  $f(x) =$

$x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ . To test here for reducibility first test for linear rational factors as before using integral factors of  $a_5$ . If there are no linear rational factors then there can be no factors of the 4th degree. Then test for quadratic rational factors as  $x^2 + b_1x + b_2$ , as above. If there are none then there can not be any rational factor of the 3rd degree. To test for the quadratic factor we divide  $f(x)$  by the quadratic and make the condition that the remainder equal zero, and then determine  $b_1$ , and  $b_2$  if possible.

$$\begin{array}{r}
 x^3 + (a_1 - b_1)x^2 + (a_2 - a_1b_1 + b_1^2 - b_2)x + a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3 \\
 x^2 + b_1x + b_2 \overline{) x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5} \\
 \underline{x^5 + b_1x^4 + b_2x^3} \\
 (a_1 - b_1)x^4 + (a_2 - b_2)x^3 + a_3x^2 + a_4x + a_5 \\
 \underline{(a_1 - b_1)x^4 + (b_1a_1 - b_1^2)x^3 + (a_1b_2 - b_1b_2)x^2} \\
 (a_2 - a_1b_1 + b_1^2 - b_2)x^3 + (a_3 - a_1b_2 + b_1b_2)x^2 + a_4x + a_5 \\
 \underline{(a_2 - a_1b_1 + b_1^2 - b_2)x^3 + (a_2b_1 - a_1b_1^2 + b_1^3 - b_1b_2)x^2 + (a_2b_2 - a_1b_1b_2 + b_1^2b_2 - b_2^2)x} \\
 (a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3)x^2 + (a_4 - a_2b_2 + a_1b_1b_2 - b_1^2b_2 + b_2^2)x + a_5 \\
 \underline{(a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3)x^2 + b_1(a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3)x} \\
 \quad + b_2(a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3) \\
 \underline{[(a_4 - a_2b_2 + a_1b_1b_2 - b_1^2b_2 + b_2^2) - b_1(a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3)]x} \\
 \quad + a_5 - b_2(a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3)
 \end{array}$$

Here we have a remainder. In order for it to vanish we must

$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$  and  $f(x)$  is reducible in  $\mathbb{R}[x]$ .  
 CAUCHY'S LEMMA APPLIED TO THE QUANTIC.

If  $a = 5$  then  $f(x) =$

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4. \text{ To test here for reducibility}$$

we first test for linear rational factors as before using  
 integral factors of  $a_4$ . If there are no linear rational factors  
 then there can be no factors of the 4th degree. Then test for  
 quadratic rational factors as  $x^2 + b_1x + b_2$ , as above. If there  
 are none then there can not be any rational factor of the 3rd  
 degree. To test for the quadratic factor we divide  $f(x)$  by the  
 quadratic and make the condition that the remainder equal zero,  
 and then determine  $b_1$  and  $b_2$  if possible.

$$\begin{aligned} & \frac{x^4 + (a_1 - b_1)x^3 + (a_2 - b_1^2 + b_1^2)x^2 + (a_3 - 2b_1b_2 + b_1^3)x + (a_4 - b_1^4 + 3b_1^2b_2 - b_1^3b_1)}{x^2 + b_1x + b_2} \\ &= (a_1 - b_1)x^2 + (a_2 - b_1^2 + b_1^2)x + (a_3 - 2b_1b_2 + b_1^3)x + (a_4 - b_1^4 + 3b_1^2b_2 - b_1^3b_1) \\ &= (a_1 - b_1)x^2 + (a_2 - b_1^2 + b_1^2)x + (a_3 - 2b_1b_2 + b_1^3)x + (a_4 - b_1^4 + 3b_1^2b_2 - b_1^3b_1) \end{aligned}$$

Here we have a remainder. In order for it to vanish we must

have

$$(1) \quad a_4 - a_2 b_2 + a_1 b_1 b_2 - b_1^2 b_2 + b_2^2 - b_1(a_3 - a_2 b_1 - a_1 b_2 + a_1 b_1^2 + 2b_1 b_2 - b_1^3) = 0$$

and

$$(2) \quad a_5 - b_2(a_3 - a_2 b_1 - a_1 b_2 + a_1 b_1^2 + 2b_1 b_2 - b_1^3) = 0$$

From (2) we get

$$a_3 - a_2 b_1 - a_1 b_2 + a_1 b_1^2 + 2b_1 b_2 - b_1^3 = \frac{a_5}{b_2}$$

Substituting in (1) we get

$$a_4 - a_2 b_2 + a_1 b_1 b_2 - b_1^2 b_2 + b_2^2 - b_1 \cdot \frac{a_5}{b_2} = 0$$

or

$$a_4 b_2 - a_2 b_2^2 + a_1 b_1 b_2^2 - b_1^2 b_2^2 + b_2^3 - a_5 b_1 = 0$$

Solving for  $b_1$ :

$$b_2^2 b_1^2 + (a_5 - a_1 b_2^2) b_1 + (a_2 b_2^2 - a_4 b_2 - b_2^3) = 0$$

$$(3) \quad b_1 = \frac{a_1 b_2^2 - a_5 \pm \sqrt{a_5^2 - 2a_1 b_2^2 a_5 + a_1^2 b_2^4 - 4a_2 b_2^4 + 4a_4 b_2^3 + 4b_2^5}}{2b_2^2}$$

To actually find the integers  $b_1$  and  $b_2$ , if there are any in the domain  $R(1)$ , take an integral factor of  $a_n = a_5$  and try it for  $b_2$  in equation (3). If it results in  $b_1$  coming out an integer then if this  $b_1$  and  $b_2$  satisfy equation (2), we have found  $x^2 + b_1 x + b_2$  and  $f(x)$ , the 5th degree polynomial is reducible in  $R(1)$ .

Example:  $f(x) \equiv x^5 + x^4 - 12x^3 - 7x^2 + 6x - 4$

To test whether this is reducible in  $R(1)$ .

have

$$(1) \quad a_4 - a_3b_2 + a_1b_2 - b_1^2 + b_2^2 - b_1(a_2 - a_1b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3) = 0$$

and

$$(2) \quad a_2 - b_2(a_2 - a_1b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3) = 0$$

From (1) we get

$$a_3 - a_2b_1 - a_1b_2 + a_1b_1^2 + 2b_1b_2 - b_1^3 = \frac{a_2}{b_2}$$

Substituting in (1) we get

$$a_4 - a_3b_2 + a_1b_2 - b_1^2 + b_2^2 - b_1 \cdot \frac{a_2}{b_2} = 0$$

or

$$a_4b_2 - a_3b_2^2 + a_1b_2^2 - b_1^2b_2 + b_2^3 - a_2b_1 = 0$$

Solving for  $b_1$ :

$$(3) \quad b_1 = \frac{a_1b_2^2 - a_2b_2 + \sqrt{a_2^2 - 2a_1a_2b_2 + a_1^2b_2^2 + 4a_1a_2b_2 + 4a_2^2}}{2b_2}$$

To actually find the integer  $b_1$  and  $b_2$ , if there are any in the domain  $R(1)$ , take an integral factor of  $a_n = a_2$  and try it for  $b_2$  in equation (3). If it results in  $b_1$  coming out an integer then it fits  $b_1$  and  $b_2$  satisfy equation (2), we have found  $x^2 = b_1x + b_2$  and  $f(x)$ , the 5th degree polynomial is reducible in  $R(1)$ .

Example:  $f(x) = x^5 - 12x^3 - 7x^2 + 6x - 4$

To test whether this is reducible in  $R(1)$ .

$$f(1) = -15 \neq 0$$

$$f(-1) = -5 \neq 0$$

$$f(2) = -68 \neq 0$$

$$f(-2) = +36 \neq 0$$

$$f(4) = -420 \neq 0$$

$$f(-4) = -140 \neq 0$$

Therefore, none of the factors of  $a_n = -4$  are roots of the equation  $f(x) = 0$ , and so there are no linear factors and no quartic factor of  $f(x)$  in  $R_1$ .

To test for a quadratic factor of form  $x^2 + b_1x + b_2$  we try a factor of  $a_n = -4$  for  $b_2$ . Let  $b_2 = -4$  and determine  $b_1$ .

$$a_1 = 1, a_2 = -12, a_3 = -7, a_4 = 6, a_5 = a_n = -4, b_2 = -4$$

$$b_1 = \frac{1(-4)^2 - (-4) \pm \sqrt{(-4)^2 - 2(1)(-4)^2 + (1)^2(-4)^4 - 4(-12)(-4)^4 + 4(6)(-4)^3 + 4(-4)^5}}{2(-4)^2}$$

$$= \frac{20 \pm \sqrt{7056}}{32} = \frac{20 \pm 84}{32} = \frac{13}{4}, -2.$$

Now if we choose  $b_1 = -2$  and  $b_2 = -4$  we find our condition (2) is satisfied.

$$(2) \quad -4 - (-4) \left[ -7 - (-12)(-2) - (1)(-4) + 1(-2)^2 + 2(-2)(-4) - (-2)^3 \right]$$

$$= -4 + 4 \left[ -31 + 32 \right] = 0$$

Therefore  $x^2 + b_1x + b_2 = x^2 - 2x - 4$  is a factor. The other factor obtained by division is  $x^3 + 3x^2 - 2x + 1$  and  $f(x) \equiv (x^2 - 2x - 4)(x^3 + 3x^2 - 2x + 1)$  and our quintic in  $R_1$  is reducible in  $R_1$ .

#### A TEST FOR IRREDUCIBILITY.

The reducibility of an equation being of prime importance we prove now another theorem which gives a test for reducibility.

$$\begin{aligned} f(1) &= -15 \neq 0 & f(-1) &= -5 \neq 0 \\ f(2) &= -38 \neq 0 & f(-2) &= +38 \neq 0 \\ f(4) &= -120 \neq 0 & f(-4) &= -120 \neq 0 \end{aligned}$$

Therefore, none of the factors of  $x^4 = -4$  are roots of the equation  $f(x) = 0$ , and so there are no linear factors and no quadratic factor of  $f(x)$  in  $R[x]$ .

To test for a quadratic factor of form  $x^2 + b_1x + b_2$  we try a factor of  $x^4 = -4$  for  $b_1$ . Let  $b_1 = -4$  and determine  $b_2$ .

$$x^4 = 1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1$$

$$x^4 = 1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1$$

$$x^2 = -1$$

$$x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1, x^2 = -1$$

Now if we choose  $b_1 = -2$  and  $b_2 = -4$  we find our condition (2) is satisfied.

$$\begin{aligned} (2) \quad & -1 - (-4) - (-2) - (-2) - (-2) - (-2) - (-2) - (-2) \\ & = -4 - 4 - 2 - 2 - 2 - 2 - 2 - 2 = 0 \end{aligned}$$

Therefore  $x^4 + b_1x + b_2 = x^4 - 2x - 4$  is a factor. The other factor obtained by division is  $x^4 + 2x - 4$  and

$$f(x) = (x^4 - 2x - 4)(x^4 + 2x - 4) \text{ and our result in } R[x] \text{ is reducible.}$$

A TEST FOR IRREDUCIBILITY.

The reducibility of an equation being of prime degree hence we prove now whether theorem which gives a test for reducibility.

Theorem: If  $p$  is a prime number, and  $a_0, a_1, a_2, \dots, a_n$  are integers, all, except  $a_0$ , divisible by  $p$ , but  $a_n$  not divisible by  $p^2$ , then

$f(x) \equiv a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$ , is irreducible.

Proof:  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ , a rational integral function.

$p$  is prime

$a_1, a_2, \dots, a_n$  are divisible by  $p$

$a_0$  is not divisible by  $p$

$a_n$  is not divisible by  $p^2$

We must show  $f(x)$  can not be factored in the rational domain.

If  $f(x)$  could be factored in the rational domain, then by Gauss's Lemma it can be factored into rational factors with integral coefficients. We would, therefore have

$$f(x) \equiv (c_0x^h + c_1x^{h-1} + \dots + c_h)(d_0x^k + d_1x^{k-1} + \dots + d_k)$$

where  $h+k = n$ , and  $c_h \cdot d_k = a_n$ , and  $c_0 \cdot d_0 = a_0$ .

Since  $a_n$  is divisible by  $p$ , therefore  $c_h \cdot d_k$  is divisible by  $p$ .

Since  $a_n$  is not divisible by  $p^2$ , therefore  $c_h$  and  $d_k$  can not both be divisible by  $p$ . Suppose  $c_h$  is the one that is divisible by  $p$  and  $d_k$  is not divisible by  $p$ .

In the factor  $c_0x^h + c_1x^{h-1} + \dots + c_h$  we have  $c_h$  divisible by  $p$ , and some other of the  $c_i$  coefficients may be divisible by  $p$ , but not all the  $c_i$  coefficients can be divisible by  $p$ , because if they were, then  $p$  would be a factor of  $f(x)$  and

Theorem: If  $p$  is a prime number, and  $a_0, a_1, a_2, \dots, a_n$  are integers, all, except  $a_0$ , divisible by  $p$ , but  $a_n$  not divisible by  $p$ , then

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n$$

is irreducible.

Proof: Let  $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ , a rational integral function.

$p$  is prime

$a_0, a_1, \dots, a_{n-1}$  are divisible by  $p$

$a_0$  is not divisible by  $p$

$a_n$  is not divisible by  $p$

We must show  $f(x)$  can not be factored in the rational domain.

If  $f(x)$  could be factored in the rational domain, then by Gauss's Lemma it can be factored into rational factors with integral coefficients. We would, therefore, have

$$f(x) = (c_0x^h + c_1x^{h-1} + \dots + c_h)(d_0x^{n-h} + d_1x^{n-h-1} + \dots + d_{n-h})$$

where  $h < n$ , and  $c_0 \cdot d_0 = a_0$ , and  $c_h \cdot d_{n-h} = a_n$ .

Since  $a_n$  is divisible by  $p$ , therefore  $c_h \cdot d_{n-h}$  is divisible by  $p$ .

Since  $a_0$  is not divisible by  $p$ , therefore  $c_0$  and  $d_0$  can not both be divisible by  $p$ . Suppose  $c_0$  is the one that is divisible by  $p$  and  $d_0$  is not divisible by  $p$ .

In the factor  $c_0x^h + c_1x^{h-1} + \dots + c_h$  we have  $c_0$  divisible by  $p$ , and some other of the  $c_i$  coefficients may be divisible by  $p$ , but not all the  $c_i$  coefficients can be divisible by  $p$ , because if they were, then  $p$  would be a factor of  $f(x)$  and

would, therefore, be a factor of  $a_0$ , which is contrary to hypothesis. Let  $c_\rho$  be the coefficient that is not divisible by  $p$  and let the others be divisible by  $p$ . Multiply out the factors of  $f(x)$  and we get for the term  $x^{h-\rho}$  the following:

$$(d_k c_\rho + d_{k-1} c_{\rho+1} + d_{k-2} c_{\rho+2} + \text{-----}) x^{h-\rho}$$

In the parenthesis here, since all the terms except  $d_k c_\rho$  are divisible by  $p$ , therefore the parenthesis is not divisible by  $p$ . But  $a_0$  is the only coefficient in  $f(x)$  which is not divisible by  $p$ , by hypothesis, therefore this parenthesis must be the coefficient  $a_0$  and, therefore,  $x^{h-\rho}$  must be  $x^n$  and, therefore,  $h-\rho = n$ . But this is impossible because  $\rho$  is a positive integer and, therefore,  $h$  would have to be greater than  $n$ , but  $h$  is actually less than  $n$  from  $h+k = n$ . Thus we have a contradiction if we assume the factors of

$f(x) \equiv (c_0 x^h + \text{-----} + c_h)(d_0 x^k + \text{-----} + d_k)$  and, therefore,  $f(x)$  is irreducible.

Thus if  $f(x) \equiv 2x^3 + 9x^2 + 6x + 12$  choose  $p = 3$ , a prime number:  $a_0 = 2$ ,  $a_1 = 9$ ,  $a_2 = 6$ ,  $a_3 = a_n = 12$ ,  $a_0$  is not divisible by 3, but  $a_1$ ,  $a_2$ , and  $a_3$  are divisible by 3, but  $a_n = a_3 = 12$  is not divisible by  $p^2 = 9$ , therefore  $f(x)$  is irreducible.

#### DEFINITION OF A CYCLOTOMIC EQUATION:

If in the equation  $x^p - 1 = 0$   $p$  is prime, and if we divide out the root 1, we get

$$\frac{x^p - 1}{x - 1} = 0 = x^{p-1} + x^{p-2} + x^{p-3} + \text{-----} + x + 1 = 0$$

would, therefore, be a factor of  $a_0$ , which is contrary to hypothesis. Let  $a_0$  be the coefficient that is not divisible by  $p$  and let the others be divisible by  $p$ . Multiply the factors of  $f(x)$  and we get for the term  $x^{n-p}$  the following:

$$(d_0 c_0 + d_1 c_1 + \dots + d_{n-p} c_{n-p}) x^{n-p}$$

In the parentheses here, since all the terms except  $d_0 c_0$  are divisible by  $p$ , therefore the parenthesis is not divisible by  $p$ . But  $a_0$  is the only coefficient in  $f(x)$  which is not divisible by  $p$ , by hypothesis, therefore this parenthesis must be the coefficient  $a_0$  and, therefore,  $x^{n-p}$  must be  $x^n$  and, therefore,  $n-p = n$ . But this is impossible because  $p$  is a positive integer and, therefore,  $p$  would have to be greater than  $n$ , but it is actually less than  $n$  from  $n-k = n$ . Thus we have a contradiction if we assume the factors of

$$f(x) = (a_0 x^n + \dots + a_1 x + a_0) (b_0 x^k + \dots + b_1 x + b_0) \text{ and, therefore, } f(x) \text{ is irreducible.}$$

$$\text{Thus if } f(x) = 2x^2 + 3x + 12 \text{ choose } p = 3, a$$

prime number:  $a_0 = 2, a_1 = 3, a_2 = 12, a_3 = 12, a_4$  is not

divisible by 3, but  $a_1, a_2$  and  $a_3$  are divisible by 3, but

$a_4 = a_3 = 12$  is not divisible by  $p = 3$ , therefore  $f(x)$  is irreducible.

#### DEFINITION OF A CYCLOTOMIC EQUATION:

If in the equation  $x^n - 1 = 0$   $p$  is prime, and if we

divide out the root 1, we get

$$\frac{x^n - 1}{x - 1} = 0 = x^{n-1} + x^{n-2} + \dots + x + 1 = 0$$

This last equation is called a cyclotomic equation.

THE CYCLOTOMIC EQUATION IS IRREDUCIBLE.

From our last theorem it is easily proven that if  $p$  is prime, then  $\frac{x^p-1}{x-1} = 0$  is irreducible in  $R_{(1)}$ , that is, the cyclotomic equation is irreducible in the domain of rational numbers. Because if we let  $x-1 = z$  and make the substitution of variable we get  $\frac{(z+1)^p-1}{z+1-1} =$

$$\frac{z^p + pz^{p-1} + \frac{p(p-1)}{2}z^{p-2} + \frac{p(p-1)(p-2)}{3}z^{p-3} + \dots + \frac{p(p-1)}{2}z^2 + pz + 1}{z} = 0$$

$$\text{or } z^{p-1} + pz^{p-2} + \frac{p(p-1)}{2}z^{p-3} + \dots + \frac{p(p-1)}{2}z + p = 0$$

Here  $a_n = p$  is prime, and all other coefficients  $a_1, a_2, \dots$  are divisible by  $p$  except  $a_0 = 1$ , and also  $a_n = p$  is not divisible by  $p^2$ , because  $p \neq 1$ , therefore this equation is irreducible and, therefore, the equation  $\frac{x^p-1}{x-1} = 0$  is irreducible. It is by use of the cyclotomic equation that Gauss showed that when  $n$  is a prime number of form  $2^k+1$  the division of a circle into  $n$  equal parts by ruler and compasses is always possible.

MULTIPLE ROOTS.

In calculus we learn that if  $f(x) = 0$  has a multiple root, then it has a common factor with  $\frac{df(x)}{dx}$  or  $f'(x)$ . This common factor can be obtained by Euclid's Algorithm. As previously mentioned, all the elements in the coefficients in the entire algorithm are in the domain of  $f(x)$  and, therefore,  $f(x)$ , if it has a multiple root can be factored into at least this

This last equation is called a cyclotomic equation.  
THE CYCLOTOMIC EQUATION IS IRREDUCIBLE.

From our last theorem it is easily proven that if  $p$

is prime, then  $\frac{x^p - 1}{x - 1} = 0$  is irreducible in  $\mathbb{R}(1)$ , that is, the cy-

clotomic equation is irreducible in the domain of rational num-

bers. Because if we let  $x - 1 = z$  and make the substitution of

$$0 = \frac{z^{p-1} + z^{p-2} + \dots + z + 1}{z} = 0$$

$$\text{or } z^{p-1} + z^{p-2} + \dots + z + 1 = 0$$

Let  $a_n = p$  is prime, and all other coefficients  $a_1, a_2, \dots, a_{n-1}$

are divisible by  $p$  except  $a_0 = 1$ , and also  $a_n = p$  is not divis-

ible by  $p$ , because  $p \nmid 1$ , therefore this equation is irreducible

and, therefore, the equation  $\frac{x^p - 1}{x - 1} = 0$  is irreducible. It is by

use of the cyclotomic equation that Gauss showed that when  $n$  is

a prime number of form  $2^k + 1$  the division of a circle into  $n$

equal parts by ruler and compass is always possible.

MULTIPLE ROOTS.

In coloring we learn that if  $f(x) = 0$  has a multiple

root, then it has a common factor with  $f'(x)$  or  $f''(x)$ . This

common factor can be obtained by Euclid's algorithm. As previ-

ously mentioned, all the elements in the coefficients in the

polynomial are in the domain of  $f(x)$  and, therefore,  $f(x)$ ,

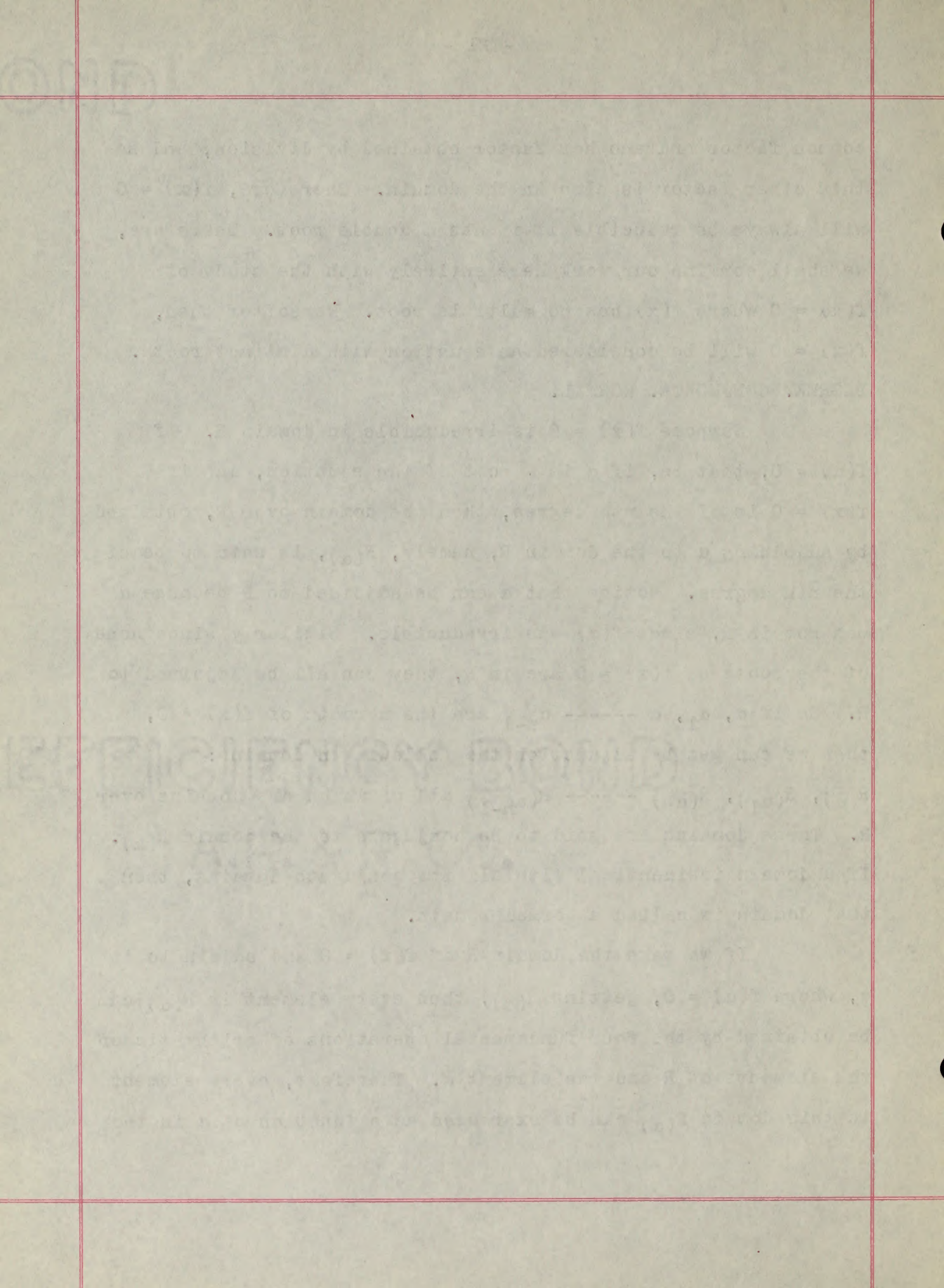
if it has a multiple root can be factored into at least this

common factor and another factor obtained by division, and so this other factor is also in the domain. Therefore,  $f(x) = 0$  will always be reducible if it has a double root. Therefore, we shall confine our work here entirely with the study of  $f(x) = 0$  where  $f(x)$  has no multiple root. Hereafter then,  $f(x) = 0$  will be considered an equation with distinct roots.

DEGREE. CONJUGATE. NORMAL.

Suppose  $f(x) = 0$  is irreducible in domain  $R$ . If  $f(\alpha) = 0$ , that is, if  $\alpha$  is a root of the equation, and if  $f(x) = 0$  is of the  $n$ th degree, then the domain over  $R$ , obtained by adjoining  $\alpha$  to the domain  $R$ , namely,  $R(\alpha)$ , is said to be of the  $n$ th degree. Notice that  $\alpha$  can be adjoined to  $R$  because  $\alpha$  was not in  $R$ , since  $f(x)$  was irreducible. Similarly since none of the roots of  $f(x) = 0$  are in  $R$ , they can all be adjoined to  $R$ . So if  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  are the  $n$  roots of  $f(x) = 0$ , then we can get by adjunction the following  $n$  domains:  $R(\alpha), R(\alpha_1), R(\alpha_2), \dots, R(\alpha_{n-1})$  all of which are domains over  $R$ . These domains are said to be conjugate to the domain  $R(\alpha)$ . If a domain is identical with all its conjugate domains, then that domain is called a Normal Domain.

If we take the domain  $R$  of  $f(x) = 0$  and adjoin to it  $\alpha$ , where  $f(\alpha) = 0$ , getting  $R(\alpha)$ , then every element in  $R(\alpha)$  can be obtained by the four fundamental operations of arithmetic on the elements of  $R$  and the element  $\alpha$ . Therefore, every element in this domain  $R(\alpha)$  can be expressed as a function of  $\alpha$  in the



domain  $R$ . As an example of this:

$$f(x) \equiv x^4 - 22x^2 + 1 = 0 \quad x^2 = \frac{22 \pm 4\sqrt{30}}{2} = 11 \pm 2\sqrt{30}$$

$$x^2 = 11 + 2\sqrt{30}$$

$$x^2 = 11 - 2\sqrt{30}$$

$$x^2 = 6 + 2\sqrt{5.6} + 5$$

$$x^2 = 6 - 2\sqrt{5.6} + 5$$

Therefore the roots are

$$\alpha = \sqrt{6} + \sqrt{5}$$

$$\alpha_2 = \sqrt{6} - \sqrt{5}$$

$$\alpha_1 = -\sqrt{6} - \sqrt{5}$$

$$\alpha_3 = -\sqrt{6} + \sqrt{5}$$

$f(x)$  is irreducible in domain  $R_{(1)}$ , domain of rationals.

$$R(1, \alpha) = R(1, \sqrt{6} + \sqrt{5})$$

$$R(1, \alpha_1) = R(1, -\sqrt{6} - \sqrt{5})$$

$$R(1, \alpha_2) = R(1, \sqrt{6} - \sqrt{5})$$

$$R(1, \alpha_3) = R(1, -\sqrt{6} + \sqrt{5})$$

$$\text{But } \alpha = -\alpha_1 \text{ because } \sqrt{6} + \sqrt{5} = -(-\sqrt{6} - \sqrt{5})$$

Therefore the adjunction of  $\alpha_1$  to  $R_{(1)}$  gives no new additional numbers that the adjunction of  $\alpha$  to  $R_{(1)}$  did not give. Similarly

$$\alpha = \frac{1}{\alpha_2} \text{ because } \sqrt{6} + \sqrt{5} = \frac{1}{(\sqrt{6} - \sqrt{5})(\sqrt{6} + \sqrt{5})} = \frac{\sqrt{6} + \sqrt{5}}{6 - 5} = \sqrt{6} + \sqrt{5}$$

therefore the adjunction of  $\alpha_2$  gives nothing new, and similarly since  $\alpha_2 = -\alpha_3$  and  $\alpha = -\frac{1}{\alpha_3}$  therefore the adjunction of  $\alpha_3$  gives nothing new and so the four domains are identical

$$R(1, \alpha) \equiv R(1, \alpha_1) \equiv R(1, \alpha_2) \equiv R(1, \alpha_3) \text{ and so the roots of } f(x)=0$$

give a normal domain, because the adjunction of each of them separately to  $R_{(1)}$  gave a set of conjugate domains all of which were identical.

Further study will show that normal domains are much easier to work with than other domains. Galois' big progress

domain  $R$ . As an example of this:

$$f(x) = x^4 - 2x^2 + 1 = 0 \quad x^2 = \frac{2 \pm 2\sqrt{3}}{2} = 1 \pm \sqrt{3}$$

$$x^2 = 1 + 2\sqrt{3} \quad x^2 = 1 - 2\sqrt{3}$$

$$x = \pm \sqrt{1 + 2\sqrt{3}} + i \quad x = \pm \sqrt{1 - 2\sqrt{3}} + i$$

Therefore the roots are

$$a = \sqrt{1 + \sqrt{3}} + \sqrt{3} \quad a_2 = \sqrt{1 - \sqrt{3}} - \sqrt{3}$$

$$a_1 = -\sqrt{1 - \sqrt{3}} - \sqrt{3} \quad a_3 = -\sqrt{1 + \sqrt{3}} + \sqrt{3}$$

$f(x)$  is irreducible in domain  $R_1$ , domain of rationals.

$$R(1, a) = R(1, \sqrt{1 + \sqrt{3}} + \sqrt{3}) \quad R(1, a_1) = R(1, -\sqrt{1 - \sqrt{3}} - \sqrt{3})$$

$$R(1, a_2) = R(1, \sqrt{1 - \sqrt{3}} - \sqrt{3}) \quad R(1, a_3) = R(1, -\sqrt{1 + \sqrt{3}} + \sqrt{3})$$

$$\text{But } a = -a_1 \text{ because } \sqrt{1 + \sqrt{3}} + \sqrt{3} = -(-\sqrt{1 - \sqrt{3}} - \sqrt{3})$$

Therefore the adjunction of  $a_1$  to  $R_1$  gives no new additional

members that the adjunction of  $a$  to  $R_1$  did not give. Similar-

$$\text{ly } a = \frac{1}{a_2} \text{ because } \sqrt{1 + \sqrt{3}} + \sqrt{3} = \frac{1}{\sqrt{1 - \sqrt{3}} - \sqrt{3}} = \frac{\sqrt{1 + \sqrt{3}} + \sqrt{3}}{1 - 3} = \sqrt{1 + \sqrt{3}}$$

Therefore the adjunction of  $a_2$  gives nothing new, and similarly

since  $a_2 = -a_3$  and  $a = -\frac{1}{a_3}$  therefore the adjunction of  $a_3$  gives

nothing new and so the four domains are identical

$$R(1, a) = R(1, a_1) = R(1, a_2) = R(1, a_3) \quad \text{and so the roots of } f(x)=0$$

give a normal domain, because the adjunction of each of them

separately to  $R_1$  gave a set of conjugate domains all of which

were identical.

Further study will show that normal domains are much

easier to work with than other domains. Galois' big program

was in the reduction of any domain to a normal domain.

CONJUGATE NUMBERS, PRIMITIVE NUMBERS, IMPRIMITIVE NUMBERS.

If  $f(x) = 0$  is irreducible in  $R$ , and its roots are  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ , then we defined  $R(\alpha), R(\alpha_1), R(\alpha_2), \dots, R(\alpha_{n-1})$  as conjugate domains. Now

if  $s$  is a function in  $R$  then

$N = s(\alpha), N_1 = s(\alpha_1), N_2 = s(\alpha_2), \dots, N_{n-1} = s(\alpha_{n-1})$  are a set of  $n$  numbers, one from each domain, and this set is called a set of conjugate numbers to  $N$ . Just as some or all of the conjugate domains may be alike, so some or all of these conjugate numbers may be equal.

If any one of these conjugate numbers is different from all its conjugates, it is called a primitive number; if it is not different from all its conjugates it is called imprimitive.

An example of this is  $f(x) = x^2 + 1 = 0$ , which is obviously irreducible in  $R(1)$ .

The roots are  $\alpha = i$ , and  $\alpha_1 = -i$ .

$R(1, i)$ , and  $R(1, -i)$  are conjugate domains and notice these domains are identical because all the elements obtainable from the four fundamental arithmetic operations on the rational numbers and  $i$  are the same as the elements obtained from using  $-i$  instead of  $+i$ , therefore  $R(1, i)$  is a normal domain. If  $s(\alpha) = a+bi = N$  where  $a$  and  $b$  are in  $R$  then  $s(\alpha_1) = a-bi = N_1$ . Here  $N$  and  $N_1$  are numbers, one from each domain and are conjugate

was in the reduction of any domain to a normal domain.

CONJUGATE NUMBERS; PRIMITIVE NUMBERS; INVARIANT NUMBERS.

If  $T(x) = 0$  is irreducible in  $R$ , and its roots are

$\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ , then we define

$R(\alpha), R(\alpha_1), R(\alpha_2), \dots, R(\alpha_{n-1})$  as conjugate domains. Now

if  $s$  is a function in  $R$  then

$s = s(\alpha), s = s(\alpha_1), s = s(\alpha_2), \dots, s = s(\alpha_{n-1})$  are a

set of  $n$  numbers, one from each domain, and this set is called

a set of conjugate numbers to  $R$ . Just as some or all of the

conjugate domains may be alike, so some or all of these conju-

gate numbers may be equal.

If any one of these conjugate numbers is different

from all the conjugates, it is called a primitive number; if it

is not different from all the conjugates it is called imprimitive.

Five.

An example of this is  $T(x) = x^2 + 1 = 0$ , which is

obviously irreducible in  $R(i)$ .

The roots are  $\alpha = i$ , and  $\alpha_1 = -i$ .

$R(i)$  and  $R(-i)$  are conjugate domains and notice

these domains are identical because all the elements obtainable

from the four fundamental arithmetic operations on the rational

numbers and  $i$  are the same as the elements obtained from using

$-i$  instead of  $i$ , therefore  $R(i)$  is a normal domain. If

$s(\alpha) = s(-\alpha) = u$  where  $\alpha$  and  $-\alpha$  are in  $R$  then  $s(\alpha) = s(-\alpha) = u$ .

Here  $u$  and  $u_1$  are numbers, one from each domain and are conjugate

numbers. They are different from each other and so are primitive numbers of the domain.

#### PRIMITIVE AND IMPRIMITIVE DOMAINS.

If a domain  $R_{(\alpha)}$  contains no imprimitive numbers excepting the numbers in  $R$ , then  $R_{(\alpha)}$  is called primitive. If  $R_{(\alpha)}$  contains imprimitive numbers besides those from  $R$ , then  $R_{(\alpha)}$  is imprimitive. That is, if the adjunction of  $\alpha$  to  $R$  did not introduce any new imprimitive numbers into the domain that were not there originally, then the new domain  $R_{(\alpha)}$  is primitive. If new imprimitive numbers were introduced, then  $R_{(\alpha)}$  is imprimitive.

#### THEOREM ON SYMMETRIC FUNCTIONS OF ROOTS.

In the study of symmetric functions in algebra a fundamental theorem is established as follows: Every rational symmetric function of the roots of an algebraic equation can be expressed rationally in terms of the coefficients.

#### THEOREM ON NUMBERS AS ROOTS OF EQUATIONS.

We shall use this theorem in the proof of the following theorem.

Theorem: Every number  $N$  in the domain  $R_{(\alpha)}$  of the  $n$ th degree is the root of some equation of the  $n$ th degree in  $R$ , the other roots of which are the remaining numbers

$N_1, N_2, N_3, \dots, N_{n-1}$  conjugate to  $N$ .

Proof: Given  $f(x) = 0$ , of  $n$ th degree in domain  $R$  with roots  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ . Let  $s$  be a function in  $R$  and

numbers. They are different from each other and so are primitive numbers of the domain.

### PRIMITIVE AND IMPRIMITIVE DOMAINS.

If a domain  $R(a)$  contains no primitive numbers except

the numbers in  $R$ , then  $R(a)$  is called primitive. If

$R(a)$  contains primitive numbers besides those from  $R$ , then

$R(a)$  is imprimitive. That is, if the adjunction of  $a$  to  $R$  did

not introduce any new primitive numbers into the domain that

were not there originally, then the new domain  $R(a)$  is primitive.

If new primitive numbers were introduced, then  $R(a)$  is imprimitive.

itive.

### THEOREM ON SYMMETRIC FUNCTIONS OF ROOTS.

In the study of symmetric functions in algebra a fundamental

theorem is established as follows: Every rational symmetric

function of the roots of an algebraic equation can be

expressed rationally in terms of the coefficients.

### THEOREM ON NUMBERS AS ROOTS OF EQUATIONS.

We shall use this theorem in the proof of the following

theorem.

Theorem: Every number  $\alpha$  in the domain  $R(a)$  of the  $n$ th

degree is the root of some equation of the  $n$ th degree in  $R$ , the

other roots of which are the remaining numbers

$\alpha_1, \alpha_2, \dots, \alpha_{n-1}$  conjugate to  $\alpha$ .

Proof: Given  $f(x) = 0$ , of  $n$ th degree in domain  $R$  with

roots  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ . Let  $a$  be a function in  $R$  and

$N = s(\alpha)$ ,  $N_1 = s(\alpha_1)$ ,  $N_2 = s(\alpha_2)$ , -----,  $N_{n-1} = s(\alpha_{n-1})$ . We will choose one of this set of conjugate numbers, say  $N$  in the domain  $R(\alpha)$ , and show it is a root of an equation of the  $n$ th degree in  $R$ , and that the conjugates of  $N$ , namely,

$N_1, N_2, \text{-----} N_{n-1}$  are the remaining roots of this equation.

Notice that domain  $R(\alpha)$  is of the  $n$ th degree because  $f(x)$  was of the  $n$ th degree and  $\alpha$  was adjoined to  $R$ . Set up the following function  $S(y)$  as the following symmetric function:

$$S(y) \equiv (y-N) (y-N_1) (y-N_2) (y-N_3) \text{-----} (y-N_{n-1}).$$

Expand and we get

$$\begin{aligned} S(y) &\equiv y^{n+(-1)^1(N+N_1+N_2+\text{-----}+N_{n-1})}y^{n-1} \\ &+(-1)^2(NN_1+NN_2+\text{----}+NN_{n-1}+N_1N_2+N_1N_3+\text{----}+N_1N_{n-1}+N_2N_3+\text{----}+N_{n-2}N_{n-1}) \\ &+(-1)^3(N_1N_2N_3+N_1N_2N_4+\text{-----}+N_{n-3}N_{n-2}N_{n-1}) \\ &+ \text{-----} \\ &+ \text{-----} \\ &+ \text{-----} \\ &+ \text{-----} + (-1)^n(NN_1N_2\text{-----}N_{n-1}) \end{aligned}$$

All the coefficients of this function in  $y$  are rational symmetric functions in  $N, N_1, N_2, \text{-----} N_{n-1}$  by preceding theorem.

But these numbers  $N, N_1, N_2, \text{-----} N_{n-1}$  are  $s$  functions in  $R$  of the  $\alpha_i$ 's. Therefore, the coefficients of  $y^i$  are symmetric



functions in  $R$  of the  $\alpha_i$ 's.

This is obvious, because if any two of the  $\alpha_i$ 's, say  $\alpha_1$  and  $\alpha_2$  are interchanged, then we simply interchange  $N_1$  and  $N_2$ , but the interchange of  $N_1$  and  $N_2$  does not change the coefficients of  $y^i$  of  $S(y)$ , so the coefficients of  $y^i$  are symmetric functions in  $R$  of the  $\alpha_i$ 's.

Since the coefficients of  $y^i$  of  $S(y)$  are symmetric functions in  $R$  of  $\alpha_i$ 's and the  $\alpha_i$ 's being roots of  $f(x) = 0$  can be expressed rationally in terms of the coefficients of  $f(x)$ , (by theorem quoted), therefore, the coefficients of  $y^i$  of  $S(y)$  can be expressed as functions in  $R$  of the coefficients of  $f(x)$ .

The coefficients of  $f(x) = 0$  are, however, elements of  $R$ , therefore the coefficients of  $y^i$ 's of  $S(y)$  are elements of  $R$ . Therefore,  $S(y) = 0$  is an equation in  $R$  of the  $n$ th degree and its roots are  $N, N_1, N_2, \dots, N_{n-1}$ .

A good example of this theorem is as follows: If we take  $f(x) = x^4 + 1 = 0$ , then the domain  $R$  of  $f(x)$  is  $R(1)$ , the domain of rationals because all the coefficients of this equation are rational numbers. The roots of  $x^4 + 1 = 0$  we find:

$$x^4 = -1; \quad x^2 = \pm i; \quad x = \pm \sqrt{i}, \pm \sqrt{-i}.$$

In polar form:  $-1 = 1 [\cos (\pi + 2 k \pi) + i \sin (\pi + 2 k \pi)]$

$$(-1)^{\frac{1}{4}} = 1^{\frac{1}{4}} \left[ \cos \frac{\pi + 2 k \pi}{4} + i \sin \frac{\pi + 2 k \pi}{4} \right]$$

$$k = 0, \alpha = 1 \left( \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = +\sqrt{i}$$

$$k = 1, \alpha_1 = 1 \left( \cos \frac{3}{4} \pi + i \sin \frac{3}{4} \pi \right) = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = +\sqrt{-i}$$

functions in  $R$  of the  $a_i$ 's.

This is obvious, because if any two of the  $a_i$ 's, say

$a_1$  and  $a_2$  are interchanged, then we simply interchange  $N_1$  and

$N_2$ , but the interchange of  $N_1$  and  $N_2$  does not change the coef-

ficients of  $y^i$  of  $S(y)$ , so the coefficients of  $y^i$  are symmetric

functions in  $R$  of the  $a_i$ 's.

Since the coefficients of  $y^i$  of  $S(y)$  are symmetric

functions in  $R$  of the  $a_i$ 's and the  $a_i$ 's being roots of  $t(x) = 0$  can

be expressed rationally in terms of the coefficients of  $t(x)$ ,

(by theorem quoted), therefore, the coefficients of  $y^i$  of  $S(y)$

can be expressed as functions in  $R$  of the coefficients of  $t(x)$ .

The coefficients of  $t(x) = 0$  are, however, elements

of  $R$ , therefore the coefficients of  $y^i$  of  $S(y)$  are elements

of  $R$ . Therefore,  $S(y) = 0$  is an equation in  $R$  of the  $n$ th degree

and its roots are  $N_1, N_2, \dots, N_{n-1}$ .

A good example of this theorem is as follows: If we

take  $t(x) = x^4 + 1 = 0$ , then the domain  $R$  of  $t(x)$  is  $R[1]$ , the

domain of rationality because all the coefficients of this equa-

tion are rational numbers. The roots of  $x^4 + 1 = 0$  we find:

$$x^4 = -1; \quad x^2 = \pm i; \quad x = \pm \sqrt{i}, \pm \sqrt{-i}.$$

In polar form:  $-1 = 1 [\cos(\pi + 2k\pi) + i \sin(\pi + 2k\pi)]$

$$(-1)^{\frac{1}{4}} = 1^{\frac{1}{4}} \left[ \cos \frac{\pi + 2k\pi}{4} + i \sin \frac{\pi + 2k\pi}{4} \right]$$

$$k = 0, \quad a = 1 \left( \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = +\sqrt{i}$$

$$k = 1, \quad a = 1 \left( \cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right) = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = +\sqrt{-i}$$

$$k = 2, \alpha_2 = 1 \left( \cos \frac{5}{4} \pi + i \sin \frac{5}{4} \pi \right) = \frac{-\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i = -\sqrt{i}$$

$$k = 3, \alpha_3 = 1 \left( \cos \frac{7}{4} \pi + i \sin \frac{7}{4} \pi \right) = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i = -\sqrt{-i}$$

Suppose  $s(\alpha) = \alpha^3 + \alpha^2 + \alpha + 1$

Then we find  $s(\alpha)$ ,  $s(\alpha_1)$ ,  $s(\alpha_2)$ , and  $s(\alpha_3)$

$$s(\alpha) = (\sqrt{i})^3 + (\sqrt{i})^2 + \sqrt{i} + 1$$

$$= i \sqrt{i} + i + \sqrt{i} + 1$$

$$= i \left( \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \right) + i + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i + 1$$

$$= \frac{\sqrt{2}}{2} i - \frac{\sqrt{2}}{2} + i + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i + 1$$

$$= \sqrt{2} i + i + 1$$

$$= 1 + (1 + \sqrt{2}) i = N$$

$$s(\alpha_1) = (\sqrt{-i})^3 + (\sqrt{-i})^2 + \sqrt{-i} + 1$$

$$= -i \sqrt{-i} - i + \sqrt{-i} + 1$$

$$= -i \left( -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i \right) - i - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i + 1$$

$$= \frac{\sqrt{2}}{2} i + \frac{\sqrt{2}}{2} - i - \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i + 1$$

$$= \sqrt{2} i - i + 1$$

$$= 1 - (1 - \sqrt{2}) i = N_1$$

$$s(\alpha_2) = (-\sqrt{i})^3 + (-\sqrt{i})^2 + (-\sqrt{i}) + 1$$

$$= -i \sqrt{i} + i - \sqrt{i} + 1$$

$$= i \left( -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i \right) + i - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i + 1$$

$$= -\frac{\sqrt{2}}{2} i + \frac{\sqrt{2}}{2} + i - \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i + 1$$

$$= -\sqrt{2} i + i + 1$$

$$= 1 + (1 - \sqrt{2}) i = N_2$$

$$k = 3, a_3 = 1 \left( \cos \frac{3}{4} \pi + i \sin \frac{3}{4} \pi \right) = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i = -\sqrt{2} i$$

$$k = 3, a_3 = 1 \left( \cos \frac{7}{4} \pi + i \sin \frac{7}{4} \pi \right) = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i = -\sqrt{2} i$$

Suppose  $s(a) = a + a + 1$   
Then we find  $s(a), s(a_1), s(a_2)$ , and  $s(a_3)$

$$s(a) = (\sqrt{2})^2 + (\sqrt{2})^2 + 1 = 1 + \sqrt{2} + 1$$

$$= 1 + \sqrt{2} + 1 + \sqrt{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= \sqrt{2} + 1 + 1 =$$

$$= 1 + (1 + \sqrt{2}) + 1 = 2$$

$$s(a_1) = (\sqrt{2})^2 + (\sqrt{2})^2 + 1 = 1 + \sqrt{2} + 1$$

$$= 1 + \sqrt{2} + 1 + \sqrt{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= \sqrt{2} + 1 + 1 =$$

$$= 1 + (1 + \sqrt{2}) + 1 = 2$$

$$s(a_2) = (\sqrt{2})^2 + (\sqrt{2})^2 + 1 = 1 + \sqrt{2} + 1$$

$$= 1 + \sqrt{2} + 1 + \sqrt{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 + 1 + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + 1 =$$

$$= \sqrt{2} + 1 + 1 =$$

$$= 1 + (1 + \sqrt{2}) + 1 = 2$$

$$s(\alpha_3) = (-\sqrt{-1})^3 + (-\sqrt{-1})^2 + (-\sqrt{-1}) + 1$$

$$= +i\sqrt{-1} - i - \sqrt{-1} + 1$$

$$= i\left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right) - i + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i + 1$$

$$= -\frac{\sqrt{2}}{2}i - \frac{\sqrt{2}}{2} - i + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i + 1$$

$$= -\sqrt{2}i - i + 1$$

$$= 1 - (1 + \sqrt{2})i = N_3$$

Take the number  $N = 1 + (1 + \sqrt{2})i$ , which is in the domain

$R(1, \alpha)$ , where  $\alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$  and this domain  $R(1, \alpha)$  contains all numbers of form  $a+bi$  where  $a$  and  $b$  are any rational number or any irrational number obtained from the four fundamental arithmetic processes on  $\sqrt{2}$ ,  $i$ . The theorem says that this number  $N$  is a root of an algebraic equation of the 4th degree in  $R(1)$ , because  $f(x) = 0$  is of the 4th degree and is in  $R(1)$ . This equation is  $S(y) = (y-N)(y-N_1)(y-N_2)(y-N_3)$ .

or

$$S(y) = [y - \{1 + (1 + \sqrt{2})i\}][y - \{1 - (1 - \sqrt{2})i\}][y - \{1 + (1 - \sqrt{2})i\}][y - \{1 - (1 + \sqrt{2})i\}] = 0$$

or

$$S(y) = [y - 1 - i - \sqrt{2}i][y - 1 + i - \sqrt{2}i][y - 1 - i + \sqrt{2}i][y - 1 + i + \sqrt{2}i] = 0$$

Multiply and we get

$$S(y) = y^4 - 4y^3 + 12y^2 - 16y + 8 = 0$$

This equation, having coefficients all rational, is in  $R(1)$ , it is of the 4th degree, just as  $f(x)$  was and  $N$  is a root. Also,  $N_1$ ,  $N_2$ ,  $N_3$ , the conjugates of  $N$  are also roots of this equation.

$$\begin{aligned} s(a_3) &= (-\sqrt{-1})^3 + (-\sqrt{-1})^2 + (-\sqrt{-1}) + 1 \\ &= -\sqrt{-1} - 1 - \sqrt{-1} + 1 \\ &= -1(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}) + (-1 + 1) + (-1 + 1) \\ &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - 1 + 1 + \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} + 1 + 1 \\ &= -\sqrt{2} - 1 + 1 \\ &= 1 - (1 + \sqrt{2}) = N_3 \end{aligned}$$

Take the number  $N = 1 + (1 + \sqrt{2})$ , which is in the domain  $R(f, a)$ , where  $a = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}$  and this domain  $R(f, a)$  contains all numbers of form  $a+bi$  where  $a$  and  $b$  are any rational number or any irrational number obtained from the four fundamental arithmetic processes on  $\sqrt{2}$ , i. e. The theorem says that this number  $N$  is a root of an algebraic equation of the 4th degree in  $R(f)$ , because  $f(x) = 0$  is of the 4th degree and is in  $R(f)$ . This

$$\text{equation is } s(y) = (y-N_1)(y-N_2)(y-N_3)(y-N_4).$$

or

$$s(y) = [y - \{1 + (1 + \sqrt{2})\}] [y - \{1 - (1 - \sqrt{2})\}] [y - \{1 - (1 - \sqrt{2})\}] [y - \{1 - (1 - \sqrt{2})\}] = 0$$

or

$$s(y) = [y - 1 - 1 - \sqrt{2}] [y - 1 - 1 - \sqrt{2}] [y - 1 + 1 + \sqrt{2}] [y - 1 + 1 + \sqrt{2}] = 0$$

Multiply and we get

$$s(y) = y^4 - 4y^3 + 12y^2 - 12y + 8 = 0$$

This equation, having coefficients all rational, is in  $R(f)$ , it is of the 4th degree, just as  $f(x)$  was and  $N$  is a root. Also,  $N_1, N_2, N_3$ , the conjugates of  $N$  are also roots of this equation.

# EVALUATION OF AN INDETERMINATE FRACTION.

We turn here to evaluate an indeterminate fraction that we shall need in the proof of the theorem that follows it. If  $f(x) = 0$  is an equation of the  $n$ th degree with no double roots, then  $f(x) = (x-a_1)(x-a_2)(x-a_3) \dots (x-a_n)$ . Then

$$\begin{aligned} \frac{df(x)}{dx} = f'(x) &= [(x-a_2)(x-a_3)\dots(x-a_n)] \\ &+ [(x-a_1)(x-a_3)(x-a_4)\dots(x-a_n)] \\ &+ \dots \\ &+ \dots \\ &+ [(x-a_1)(x-a_2)(x-a_3)\dots(x-a_{n-1})] \end{aligned}$$

or

$$\begin{aligned} f'(x) &= \frac{f(x)}{x-a_1} + \frac{f(x)}{x-a_2} + \frac{f(x)}{x-a_3} + \dots + \frac{f(x)}{x-a_n} \\ \therefore f'(a_1) &= \frac{f(a_1)}{a_1-a_1} + \frac{f(a_1)}{a_1-a_2} + \frac{f(a_1)}{a_1-a_3} + \dots + \frac{f(a_1)}{a_1-a_n} \end{aligned}$$

But  $f(a_1) = 0$ , and  $a_1-a_2 \neq 0$ ,  $a_1-a_3 \neq 0$ ,  $\dots$ ,  $a_1-a_n \neq 0$ , because there are no double roots, therefore, all the fractions except the first are equal to zero, and we have

$$f'(a_1) = \frac{f(a_1)}{a_1-a_1} + 0 + 0 + \dots + 0 \therefore$$

the indeterminate form  $\frac{0}{0} = \frac{f(a_1)}{a_1-a_1} = f'(a_1)$  or

$$\lim_{x \rightarrow a_1} \frac{f(x)}{x-a_1} = f'(a_1), \text{ where } f(a_1) = 0.$$

We shall use this result in the following theorem.

# EVALUATION OF AN INDETERMINATE FRACTION.

We turn here to evaluate an indeterminate fraction that we shall need in the proof of the theorem that follows it. If  $f(x) = 0$  is an equation of the  $n$ th degree with no double roots, then  $f(x) = (x-a_1)(x-a_2) \cdots (x-a_n)$ . Then

$$\frac{f'(x)}{f(x)} = \frac{f'(x)}{(x-a_1)(x-a_2) \cdots (x-a_n)} = \frac{f'(x)}{(x-a_1)} \cdot \frac{1}{(x-a_2) \cdots (x-a_n)} + \frac{f'(x)}{(x-a_2)} \cdot \frac{1}{(x-a_1) \cdots (x-a_n)} + \cdots + \frac{f'(x)}{(x-a_n)} \cdot \frac{1}{(x-a_1) \cdots (x-a_{n-1})}$$

or

$$\frac{f'(x)}{f(x)} = \frac{f'(x)}{x-a_1} + \frac{f'(x)}{x-a_2} + \cdots + \frac{f'(x)}{x-a_n}$$

$$\therefore \frac{f'(a_1)}{f(a_1)} = \frac{f'(a_1)}{a_1-a_1} + \frac{f'(a_1)}{a_1-a_2} + \cdots + \frac{f'(a_1)}{a_1-a_n}$$

But  $f(a_1) = 0$ , and  $a_1-a_2 \neq 0$ ,  $a_1-a_3 \neq 0$ ,  $\cdots$ ,  $a_1-a_n \neq 0$ , because there are no double roots, therefore, all the fractions except the first are equal to zero, and we have

$$\frac{f'(a_1)}{f(a_1)} = \frac{f'(a_1)}{a_1-a_1} + 0 + 0 + \cdots + 0$$

the indeterminate form  $\frac{0}{0} = \frac{f'(a_1)}{a_1-a_1} = f'(a_1)$  or

$$\lim_{x \rightarrow a_1} \frac{f'(x)}{f(x)} = f'(a_1), \text{ where } f(a_1) = 0.$$

We shall use this result in the following theorem.

# THEOREM ON THE FUNCTION OF ANY PRIMITIVE NUMBER.

Theorem: Every number of the domain  $R_{(\alpha)}$  can be expressed as a function in  $R$  of any primitive number  $N$  of the domain  $R_{(\alpha)}$ .

Proof: As before  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  are the roots of the irreducible  $f(x) = 0$ , and  $s$  is a function in  $R$ , and  $s(\alpha) = N, s(\alpha_1) = N_1, s(\alpha_2) = N_2, \dots, s(\alpha_{n-1}) = N_{n-1}$  are  $n$  conjugate numbers in  $n$  domains, and choose  $N$  in  $R_{(\alpha)}$  as a primitive number, so that it is different from all its conjugates.

Let  $M$  be any number in the domain  $R_{(\alpha)}$  and  $M_1, M_2, M_3, \dots, M_{n-1}$  be its conjugates, so that here we have another set of conjugate numbers in  $n$  domains, all the numbers coming from some same function in  $R$ .

Set up  $S(x) \equiv (x-N)(x-N_1)(x-N_2) \dots (x-N_{n-1})$ .

Also set up a function

$$T(x) \equiv \frac{MS(x)}{x-N} + \frac{M_1S(x)}{x-N_1} + \frac{M_2S(x)}{x-N_2} + \dots + \frac{M_{n-1}S(x)}{x-N_{n-1}}$$

Since  $S(x)$  is of the  $n$ th degree this  $T(x)$  function is of the  $n-1$  degree.

Suppose now we interchange any two of the  $\alpha_i$ 's, as  $\alpha_1$  and  $\alpha_2$ ; then from  $s(\alpha_1) = N_1$  and  $s(\alpha_2) = N_2$  we see we are interchanging  $N_1$  and  $N_2$ . Also, since  $M_1$  and  $M_2$  came both from some function in  $R$ , and both came from the same function on  $\alpha_1$  and  $\alpha_2$ , therefore we are also interchanging  $M_1$  and  $M_2$ . But  $S(x)$  is not altered in any way, the order of the factors is

THEOREM ON THE FACTOR OF ANY PRIMITIVE FUNCTION.

Theorem: Every number of the domain  $R(a)$  can be expressed as a function in  $R$  of any primitive number  $N$  of the domain  $R(a)$ .

Proof: As before  $a, a_1, a_2, \dots, a_{n-1}$  are the roots of the irreducible  $f(x) = 0$ , and  $s$  is a function in  $R$ , and  $s(a) = N, s(a_1) = N_1, s(a_2) = N_2, \dots, s(a_{n-1}) = N_{n-1}$  are  $n$  conjugate numbers in a domain, and choose  $N$  and  $N_{n-1}$  as a primitive number, so that it is different from all its conjugates.

Let  $N$  be any number in the domain  $R(a)$ , and  $N_1, N_2, \dots, N_{n-1}$  be its conjugates, so that here we have another set of conjugate numbers in a domain, all the numbers coming from some function in  $R$ .

$$\text{Set up } S(x) = (x-N)(x-N_1)(x-N_2)\dots(x-N_{n-1}).$$

Also set up a function

$$T(x) = \frac{N_2 S(x)}{x-N_2} + \frac{N_3 S(x)}{x-N_3} + \dots + \frac{N_{n-1} S(x)}{x-N_{n-1}} + \frac{N_1 S(x)}{x-N_1}$$

Since  $S(x)$  is of the  $n$ th degree this  $T(x)$  function is of the  $n-1$  degree.

Suppose now we interchange any two of the  $a_i$ 's, as

$a_1$  and  $a_2$ ; then from  $s(a_1) = N_1$  and  $s(a_2) = N_2$  we see we are interchanging  $N_1$  and  $N_2$ . Also, since  $N_1$  and  $N_2$  came both from some function in  $R$ , and both came from the same function on  $a_1$  and  $a_2$ , therefore we are also interchanging  $N_1$  and  $N_2$ . But  $S(x)$  is not altered in any way, the order of the factors is

merely interchanged. So in  $T(x)$  we are merely interchanging two fractions, in this case the second and third fractions. In other words, the interchange of any two  $\alpha_i$ 's interchanges merely two fractions in  $T(x)$ , but  $T(x)$  is not affected by this. So  $T(x)$  is a symmetric function of the  $\alpha_i$ 's in  $R$  and the coefficients of  $T(x)$  are numbers in  $R$ .

If in  $S(x)$  and  $T(x)$  we let  $x = N$ , we get

$$S(N) = (N-N) (N-N_1) \text{ ----- } (N-N_{n-1}) = 0 \text{ and}$$

$$T(N) = \frac{MS(N)}{N-N} + \frac{M_1S(N)}{N-N_1} + \frac{M_2S(N)}{N-N_2} + \text{-----} + \frac{M_{n-1}S(N)}{N-N_{n-1}}$$

Since  $S(N) = 0$ , therefore the numerators of these fractions are zero. Since  $N$  is primitive by hypothesis, therefore it differs from all the other  $N_i$  so

$$N-N_1 \nmid 0, N-N_2 \nmid 0, \text{-----}, N-N_{n-1} \nmid 0.$$

Each fraction in  $T(N)$  except the first one is, therefore, equal to zero. The first one  $\frac{MS(N)}{N-N} = \frac{0}{0}$ , is an indeterminate fraction. Now applying the preceding theorem, which we just proved, to this indeterminate form, we have

$$\lim_{x \rightarrow N} \frac{S(x)}{x-N} = S'(N) \text{ where } S'(N) = \left[ \frac{dS(x)}{dx} \right]_{x=N}$$

$$\therefore \frac{S(N)}{N-N} = S'(N)$$

$$\text{So } \frac{MS(N)}{N-N} = MS'(N)$$

If now in  $T(x)$  we let  $x = N$  we have

$$T(N) = \frac{MS(N)}{N-N} = MS'(N) \text{ or } M = \frac{T(N)}{S'(N)}.$$

merely interchanged. So in  $T(x)$  we are merely interchanging two fractions, in this case the second and third fractions. In other words, the interchange of any two  $a_i$ 's interchanges merely two fractions in  $T(x)$ , but  $T(x)$  is not affected by this. So  $T(x)$  is a symmetric function of the  $a_i$ 's in  $R$  and the coefficients of  $T(x)$  are numbers in  $R$ .

It is in  $S(x)$  and  $T(x)$  we let  $x = W$ , we get

$$S(W) = (W-N_1)(W-N_2) \cdots (W-N_{n-1}) = 0 \text{ and}$$

$$T(W) = \frac{M_1 S(W)}{W-N_1} + \frac{M_2 S(W)}{W-N_2} + \cdots + \frac{M_{n-1} S(W)}{W-N_{n-1}}$$

Since  $S(W) = 0$ , therefore the numerators of these fractions are zero. Since  $W$  is primitive by hypothesis, therefore it differs from all the other  $N_i$  so

$$W-N_i \neq 0, \quad W-N_i \neq 0, \quad \cdots, \quad W-N_{n-1} \neq 0.$$

Each fraction in  $T(W)$  except the first one is, therefore, equal to zero. The first one  $\frac{M_1 S(W)}{W-N_1}$  is an indeterminate fraction. Now applying the preceding theorem, which we have just proved, to this indeterminate form, we have

$$\lim_{x \rightarrow W} \frac{S(x)}{x-W} = S'(W) \text{ where } S'(W) = \frac{dS(x)}{dx} \Big|_{x=W}$$

$$\therefore \frac{S(W)}{W-N_1} = S'(W)$$

$$\text{So } \frac{M_1 S(W)}{W-N_1} = M_1 S'(W)$$

It is now in  $T(x)$  we let  $x = W$  we have

$$T(W) = \frac{M_1 S(W)}{W-N_1} + M_2 S'(W) + \cdots + M_{n-1} S'(W)$$

Here  $S'(N) \neq 0$  because  $S(x)$  has no multiple roots.

We have thus shown that any number  $M$  of the domain  $R(\alpha)$  can be expressed as a function in  $R$  of any primitive number  $N$  of the domain  $R(\alpha)$ , because both  $T(N)$  and  $S'(N)$  are functions of  $N$  in  $R$ .

# THEOREM ON CONJUGATE NUMBERS AS ROOTS OF AN IRREDUCIBLE EQUATION.

Theorem: If  $N$  is primitive in  $R(\alpha)$ , then the set of conjugate numbers,  $N, N_1, N_2, \dots, N_{n-1}$ , are roots of an irreducible equation in  $R, S(x) = 0$ , of the  $n$ th degree.

By hypothesis we have  $f(x) = 0$ , an  $n$ th degree irreducible equation in  $R$ , its roots  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ ;  $s$  is a function in  $R, N = s(\alpha), N_1 = s(\alpha_1), \dots, N_{n-1} = s(\alpha_{n-1})$  a set of conjugate numbers and  $N$  in  $R(\alpha)$  is primitive so that it differs from all the other  $N_i$ .

Set up equation  $S(x) \equiv (x-N)(x-N_1) \dots (x-N_{n-1}) = 0$ . This is of the  $n$ th degree and applying a previous theorem:

"Every number  $N$  in the domain  $R(\alpha)$  of the  $n$ th degree is the root of some equation of the  $n$ th degree in  $R$ , the other roots of which are the remaining numbers conjugate to  $N$ , namely,

$N_1, N_2, \dots, N_{n-1}$ , so we have shown that this  $S(x) = 0$  is an equation of the  $n$ th degree in  $R$ . If  $S(x) = 0$  is irreducible, then our theorem is proven. So assume  $S(x) = 0$  is reducible and write it in its lowest degree factors where each factor is in  $R$  and is irreducible itself, as

$$S(x) = U(x) \cdot U_1(x) \cdot U_2(x) \dots U_m(x) = 0$$

Let  $S'(N) \neq 0$  be the sum of the roots.

We have then shown that any number  $N$  of the domain  $R(N)$  can be expressed as a function in  $R$  of any primitive number  $N$  of the domain  $R(N)$ , because both  $T(N)$  and  $S'(N)$  are functions of  $N$  in

### THEOREM ON CONJUGATE NUMBERS AS ROOTS OF AN IRREDUCIBLE EQUATION

Theorem: If  $N$  is primitive in  $R(N)$ , then the set of

conjugate numbers,  $N, N_1, N_2, \dots, N_{n-1}$ , are roots of an irre-

ducible equation in  $R, S(x) = 0$ , of the  $n$ th degree.

By hypothesis we have  $T(x) = 0$ , an  $n$ th degree irre-

ducible equation in  $R$ , its roots  $N, N_1, N_2, \dots, N_{n-1}$ ;  $N$  is a

function in  $R, N = S(N), N_1 = S(N_1), N_2 = S(N_2), \dots, N_{n-1} = S(N_{n-1})$  a set

of conjugate numbers and  $N$  in  $R(N)$  is primitive so that it dif-

fers from all the other  $N_i$ .

Set up equation  $S(x) \equiv (x-N)(x-N_1) \dots (x-N_{n-1}) = 0$ .

This is of the  $n$ th degree and applying a previous theorem:

Every number  $N$  in the domain  $R(N)$  of the  $n$ th degree is the root

of some equation of the  $n$ th degree in  $R$ , the other roots of which

are the remaining numbers conjugate to  $N$ , namely,

$N_1, N_2, \dots, N_{n-1}$ , so we have shown that this  $S(x) = 0$  is an

equation of the  $n$ th degree in  $R$ . If  $S(x) = 0$  is irreducible,

then the theorem is proved. We assume  $S(x) = 0$  is reducible and

write it in its lowest degree factors where each factor is in  $R$

and is irreducible itself, as

$$S(x) = U(x) \cdot U_1(x) \cdot U_2(x) \cdot \dots \cdot U_g(x) = 0$$

where each  $U_i$  function is irreducible in  $R$ . Take any one of these irreducible factors, as  $U(x)$ . Then  $U(x) = 0$  must have as a root at least one of the numbers which are roots of  $S(x) = 0$  in order to make it,  $U(x)$ , vanish. So at least one of the numbers  $N, N_1, N_2, \dots, N_{n-1}$  is a root of  $U(x) = 0$ . Suppose  $N_1$  is such a root. So that  $U(N_1) = 0$ . But  $N_1 = s(\alpha_1)$  by hypothesis. Therefore, substituting we get  $U[s(\alpha_1)] = 0$ . Here we see  $\alpha_1$  is one of the roots of  $U[s(\alpha_1)] = 0$ . But  $\alpha_1$  is a root of the irreducible  $f(x)$  by hypothesis, so  $U[s(\alpha_1)] = 0$  and  $f(x) = 0$  are two algebraic equations with a common root,  $\alpha_1$ .

We have proven "If two equations are in domain  $R$ , and one is irreducible in  $R$ , and this irreducible equation has one root which satisfies the other equation, then all the roots of the irreducible equation satisfy the other equation." So since  $f(x) = 0$  and  $U[s(\alpha_1)] = 0$  are two equations in  $R$ , and  $f(x) = 0$  is irreducible in  $R$ , and  $f(x) = 0$  has one root  $\alpha_1$ , which satisfies  $U[s(\alpha_1)] = 0$ , therefore all the roots of  $f(x) = 0$ , namely,  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ , satisfy  $U[s(\alpha_1)] = 0$ , therefore  $U[s(\alpha)] = 0, U[s(\alpha_1)] = 0, U[s(\alpha_2)] = 0, \dots, U[s(\alpha_{n-1})] = 0$ . But, since  $N = s(\alpha), N_1 = s(\alpha_1), N_2 = s(\alpha_2), \dots, N_{n-1} = s(\alpha_{n-1})$ ; therefore, by substitution  $U(N) = 0, U(N_1) = 0, U(N_2) = 0, \dots, U(N_{n-1}) = 0$ , therefore since one of the  $N_i$  is a root of  $U(x) = 0$ , therefore all the  $N_i$  are roots of  $U(x) = 0$ .

If  $N, N_1, N_2, \dots, N_{n-1}$  by hypothesis are all distinct, then  $U(x) = 0$  is of the  $n$ th degree and  $S(x)$  and  $U(x)$  are identical. By hypothesis  $U(x) = 0$  is irreducible. Therefore,

where each  $U_i$  is irreducible in  $R$ . Take any one of these irreducible factors, say  $U(x)$ . Then  $U(x) = 0$  must have as a root at least one of the numbers which are roots of  $S(x) = 0$  in order to make it,  $U(x)$ , vanish. So at least one of the numbers  $N_1, N_2, \dots, N_{n-1}$  is a root of  $U(x) = 0$ . Suppose  $N_1$  is such a root. So that  $U(N_1) = 0$ . But  $N_1 = u(a_1)$  by hypothesis. Therefore, substituting we get  $U[u(a_1)] = 0$ . Here we see  $u_1$  is one of the roots of  $U[u(a_1)] = 0$ . But  $u_1$  is a root of the irreducible  $f(x)$  by hypothesis, so  $U[u(a_1)] = 0$  and  $f(x) = 0$  are two algebraic equations with a common root,  $u_1$ .

We have proven "If two equations are in domain  $R$ , and one is irreducible in  $R$ , and this irreducible equation has one root which satisfies the other equation, then all the roots of the irreducible equation satisfy the other equation." So since  $f(x) = 0$  and  $U[u(a_1)] = 0$  are two equations in  $R$ , and  $f(x) = 0$  is irreducible in  $R$ , and  $f(x) = 0$  has one root  $u_1$ , which satisfies  $U[u(a_1)] = 0$ , therefore all the roots of  $f(x) = 0$ , namely,

$u_1, u_2, \dots, u_{n-1}$ , satisfy  $U[u(a_1)] = 0$ , therefore  $U[u(a_1)] = 0, U[u(a_2)] = 0, \dots, U[u(a_{n-1})] = 0$ . But, since  $N = u(a_1), N_2 = u(a_2), \dots, N_{n-1} = u(a_{n-1})$ , therefore, by substitution  $U(N) = 0, U(N_2) = 0, \dots, U(N_{n-1}) = 0$ , therefore since one of the  $N_i$  is a root of  $U(x) = 0$ , therefore all the  $N_i$  are roots of  $U(x) = 0$ .

If  $N, N_1, N_2, \dots, N_{n-1}$  by hypothesis are all distinct, then  $U(x) = 0$  is of the  $n$ th degree and  $S(x)$  and  $U(x)$  are identical. By hypothesis  $U(x) = 0$  is irreducible. Therefore,

$S(x) = 0$  is irreducible.

# NORMAL EQUATIONS.

If in an equation, irreducible in  $R$ , each root can be expressed as a function in  $R$  of one of the roots, that equation is called a Normal Equation.

Example:  $x^4 + 1 = 0$ . This is irreducible in  $R_{(1)}$ .

The roots are  $\alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$

$$\alpha_1 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$$

$$\alpha_2 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$$

$$\alpha_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$$

$$\alpha_1 = -\alpha$$

$$\alpha_2 = -(\alpha^3) = -\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i\right)^3 = -\left[\frac{\sqrt{2}}{4} + \frac{3\sqrt{2}}{4} i - \frac{3\sqrt{2}}{4} - \frac{\sqrt{2}}{4} i\right] = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2} i$$

$$\alpha_3 = (\alpha^3) = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i\right)^3 = \frac{\sqrt{2}}{4} + \frac{3\sqrt{2}}{4} i - \frac{3\sqrt{2}}{4} - \frac{\sqrt{2}}{4} i = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i$$

$\therefore$  since  $x^4 + 1 = 0$  is irreducible and three of its roots,

$\alpha_1, \alpha_2, \alpha_3$ , are expressible in  $R_{(1)}$  as functions of the fourth root  $\alpha$ ,  $\therefore x^4 + 1 = 0$  is Normal.

## THEOREM ON PRIMITIVE NUMBERS AS ROOTS OF NORMAL EQUATIONS.

A primitive number of a normal domain of the  $n$ th degree is a root of a normal equation of the  $n$ th degree.

Let  $N$  be any primitive number in the normal domain  $R_{(p)}$  where  $R_{(p)}$  is a domain of the  $n$ th degree, obtained by adjunction of  $p$  to the domain  $R$ . We have proven that every  $N$  in

$$3(x) = 0 \text{ is irreducible.}$$

# NORMAL EQUATIONS

It is an equation, irreducible in  $K$ , each root can be expressed as a function in  $K$  of one of the roots, that equation is called a Normal Equation.

Example:  $x^4 + 1 = 0$ . This is irreducible in  $\mathbb{R}(i)$ .

$$\text{The roots are } \alpha = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$

$$\alpha_1 = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

$$\alpha_2 = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i$$

$$\alpha_3 = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$

$$\alpha_1 = -\alpha$$

$$\alpha_2 = -(\alpha^3) = -\left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^3 = -\left[\frac{\sqrt{2}}{2} + \frac{3\sqrt{2}}{4}i - \frac{3\sqrt{2}}{4}i - \frac{\sqrt{2}}{2}\right] = -\frac{\sqrt{2}-\sqrt{2}}{2}$$

$$\alpha_3 = (\alpha^2) = \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)^2 = \frac{\sqrt{2}}{2} + \frac{3\sqrt{2}}{4}i - \frac{3\sqrt{2}}{4}i - \frac{\sqrt{2}}{2} = -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$

$\therefore$  since  $x^4 + 1 = 0$  is irreducible and three of its roots,

$\alpha_1, \alpha_2, \alpha_3$  are expressible in  $\mathbb{R}(i)$  as functions of the fourth

root  $\alpha$ ,  $\therefore x^4 + 1 = 0$  is Normal.

## THEOREM ON IRREDUCIBLE ROOTS OF NORMAL EQUATIONS

A primitive number of a normal domain of the  $n$ th de-

gree is a root of a normal equation of the  $n$ th degree.

Let  $N$  be any primitive number in the normal domain

$\mathbb{R}(p)$  where  $\mathbb{R}(p)$  is a domain of the  $n$ th degree, obtained by ad-

junction of  $p$  to the domain  $\mathbb{R}$ . We have proven that every  $N$  in

the domain  $R_{(p)}$  of the  $n$ th degree is the root of some equation of the  $n$ th degree in  $R$ , the other roots of which are the remaining numbers conjugate to  $N$ , namely,  $N_1, N_2, \dots, N_{n-1}$ , where  $N = s(p), N_1 = s(p_1), N_2 = s(p_2), \dots, N_{n-1} = s(p_{n-1})$ , and  $s$  is a function in  $R$ . So by this theorem  $N$ , any number in  $R_{(p)}$  is a root of an equation of the  $n$ th degree in  $R$ , say the equation  $S(x) = 0$ . So  $S(x) = 0$  is an  $n$ th degree equation in  $R$  with roots  $N, N_1, N_2, \dots, N_{n-1}$ . Also  $S(x) = 0$  is irreducible because we proved that if  $N$  is primitive in  $R_{(p)}$  then the numbers  $N, N_1, N_2, \dots, N_{n-1}$  are roots of an irreducible equation of the  $n$ th degree.

Since  $N = s(p)$ , therefore  $N$  is in domain  $R_{(p)}$ .

Since  $N_1 = s(p_1)$ , therefore  $N_1$  is in domain  $R_{(p_1)}$ , etc.

Since  $N_{n-1} = s(p_{n-1})$ , therefore  $N_{n-1}$  is in domain  $R_{(p_{n-1})}$ .

But by hypothesis  $R_{(p)}$  is a normal domain so it is identical with its conjugate domains by definition, therefore  $R_{(p)} = R_{(p_1)} = \dots = R_{(p_{n-1})}$ . So all the numbers  $N, N_1, N_2, \dots, N_{n-1}$  belong to the identically same domain  $R_{(p)}$ . But we have also proved that every number of the domain  $R_{(p)}$  can be expressed as a function in  $R$  of any primitive number  $N$  of the domain  $R_{(p)}$ . So every number  $N, N_1, N_2, \dots, N_{n-1}$ , can be expressed as a function in  $R$  of the primitive number  $N$ . But  $S(x) = 0$  is of the  $n$ th degree, and is irreducible and its roots  $N, N_1, N_2, \dots, N_{n-1}$  can be expressed as a function in  $R$  of one of the roots,  $N$ , therefore  $S(x) = 0$  is a normal equation.

the domain  $R(p)$  of the  $n$ th degree is the root of some equation of the  $n$ th degree in  $R$ , the other roots of which are the remaining numbers conjugate to  $\alpha$ , namely,  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ , where  $\alpha = \alpha(p)$ ,  $\alpha_1 = \alpha(p_1)$ ,  $\alpha_2 = \alpha(p_2)$ ,  $\dots$ ,  $\alpha_{n-1} = \alpha(p_{n-1})$ , and  $\alpha$  is a function in  $R$ . So by this theorem, any number in  $R(p)$  is a root of an equation of the  $n$ th degree in  $R$ , say the equation  $S(x) = 0$ . So  $S(x) = 0$  is an  $n$ th degree equation in  $R$  with roots  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$ . Also  $S(x) = 0$  is irreducible because we proved that if  $W$  is primitive in  $R(p)$  then the numbers  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  are roots of an irreducible equation of the  $n$ th degree.

Since  $\alpha = \alpha(p)$ , therefore  $\alpha$  is in domain  $R(p)$ .  
Since  $\alpha_1 = \alpha(p_1)$ , therefore  $\alpha_1$  is in domain  $R(p_1)$ , etc.  
Since  $\alpha_{n-1} = \alpha(p_{n-1})$ , therefore  $\alpha_{n-1}$  is in domain  $R(p_{n-1})$ .

But by hypothesis  $R(p)$  is a normal domain so it is identical with the conjugate domain by definition, therefore  $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$  belong to the domain  $R(p)$ . So all the numbers  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  belong to the domain  $R(p)$ . But we have also proved that every number of the domain  $R(p)$  can be expressed as a function in  $R$  of any primitive number  $\alpha$  of the domain  $R(p)$ . So every number  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  can be expressed as a function in  $R$  of the primitive number  $\alpha$ . But  $S(x) = 0$  is of the  $n$ th degree, and is irreducible and its roots  $\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1}$  can be expressed as a function in  $R$  of one of the roots,  $\alpha$ , therefore  $S(x) = 0$  is a normal equation.

## THE GALOIS DOMAIN.

If any equation is in the domain  $R$ , then the domain obtained by adjunction of all the distinct roots of the equation to  $R$  is called the Galois Domain of the equation. Thus, if  $f(x) = 0$  is in the domain  $R$ , of the  $n$ th degree with the  $n$  distinct roots  $\alpha, \alpha_1, \dots, \alpha_{n-1}$ , then  $R(\alpha, \alpha_1, \alpha_2, \dots, \alpha_{n-1})$  is called the Galois Domain of  $f(x) = 0$ . It can be shown that the adjunction of several magnitudes to a domain may be replaced by the adjunction of a single magnitude. Thus, to obtain the Galois domain for an equation it is not always necessary to adjoin all the roots, but a single magnitude may be found which can replace the adjoining all the roots and will give a domain which will include all the elements obtainable if all the roots had been adjoined.

An example of the Galois Domain:

$$f(x) \equiv x^5 - 2x^4 - 2x^3 + x^2 - 3x + 6 = 0$$

$$(x - 2)(x^4 - 2x^2 - 3) = 0$$

$$(x - 2)(x^2 - 3)(x^2 + 1) = 0$$

$$x = 2, +\sqrt{3}, -\sqrt{3}, +i, -i$$

$f(x)$  is in domain  $R_{(1)}$ , the domain of rationals.

The root 2 is already in  $R_{(1)}$ .

The roots  $+\sqrt{3}$  and  $-\sqrt{3}$  will not give different elements so we need adjoin only  $\sqrt{3}$ .

Similarly for  $i$  and  $-i$ .

Therefore  $R_{(1, \sqrt{3}, i)}$  is the Galois Domain for  $f(x)$ .

Another example of the Galois Domain:

# THE GALOIS DOMAIN.

If any equation is in the domain  $R$ , then the domain obtained by adjunction of all the distinct roots of the equation to  $R$  is called the Galois Domain of the equation. Thus, if  $f(x) = 0$  is in the domain  $R$ , of the adjunction with the

distinct roots  $\alpha_1, \alpha_2, \dots, \alpha_n$ , then  $R(\alpha_1, \alpha_2, \dots, \alpha_n)$  is called the Galois Domain of  $f(x) = 0$ . It can be shown that

the adjunction of several equations to a domain may be replaced by the adjunction of a single equation. Thus, to obtain the Galois Domain for an equation it is not always necessary to adjoint all the roots, but a single equation may be

found which can replace the adjoining all the roots and will give a domain which will include all the elements obtainable if all the roots had been adjoined.

An example of the Galois Domain:

$$f(x) = x^5 - 2x^4 - 3x^3 + x^2 - 3x + 6 = 0$$

$$(x - 2)(x^4 - 2x^3 - 5x^2 + 6x - 3) = 0$$

$$(x - 2)(x^2 - 3)(x^2 + 1) = 0$$

$$x = 2, \sqrt{3}, -\sqrt{3}, i, -i$$

$f(x)$  is in domain  $R_1$ , the domain of rationals.

The root 2 is already in  $R_1$ .

The roots  $\sqrt{3}$  and  $-\sqrt{3}$  will not give different elements

so we need adjoin only  $\sqrt{3}$ .

Similarly for  $i$  and  $-i$ .

Therefore  $R_1(\sqrt{3}, i)$  is the Galois Domain for  $f(x)$ .

Another example of the Galois Domain:

$$\text{Given } f(x) \equiv \frac{x^5-1}{x-1} = x^4 + x^3 + x^2 + x + 1 = 0.$$

Since this is a cyclotomic equation, we have already proven that it is irreducible. We shall find its roots.

Since  $x \neq 0$ , divide by  $x^2$  getting

$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$ . This is a reciprocal equation. To solve it, rewrite it, adding 1 to each side.

$$x^2 + 2 + \frac{1}{x^2} + x + \frac{1}{x} = 1$$

$$\text{let } x + \frac{1}{x} = z$$

$$x^2 + 2 + \frac{1}{x^2} = z^2$$

Substitute, get  $z^2 + z - 1 = 0$

$$z = \frac{-1 \pm \sqrt{5}}{2}$$

$$x + \frac{1}{x} = \frac{-1 + \sqrt{5}}{2}$$

$$x + \frac{1}{x} = \frac{-1 - \sqrt{5}}{2}$$

$$x^2 - \frac{-1 + \sqrt{5}}{2} x + 1 = 0$$

$$x^2 + \frac{1 + \sqrt{5}}{2} x + 1 = 0$$

$$x = \frac{\frac{-1 + \sqrt{5}}{2} \pm \sqrt{\frac{3 - \sqrt{5}}{2} - 4}}{2}$$

$$x = \frac{\frac{-1 - \sqrt{5}}{2} \pm \sqrt{\frac{3 + \sqrt{5}}{2} - 4}}{2}$$

$$x = -\frac{1}{4} + \frac{\sqrt{5}}{4} \pm \frac{1}{4} \sqrt{-10 - 2\sqrt{5}}$$

$$x = -\frac{1}{4} - \frac{\sqrt{5}}{4} \pm \sqrt{-10 + 2\sqrt{5}}$$

$$x = -\frac{1}{4} + \frac{\sqrt{5}}{4} \pm \frac{1}{4} i \sqrt{10 + 2\sqrt{5}}$$

$$x = -\frac{1}{4} - \frac{\sqrt{5}}{4} \pm i \frac{1}{4} \sqrt{10 - 2\sqrt{5}}$$

The four roots are therefore:

$$\alpha = -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} i \sqrt{10 + 2\sqrt{5}}$$

$$\alpha_1 = -\frac{1}{4} + \frac{\sqrt{5}}{4} - \frac{1}{4} i \sqrt{10 + 2\sqrt{5}}$$

$$\text{Given } f(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1 = 0.$$

Since this is a cubic equation, we have already

proved that it is irreducible. We shall find its roots.

Since  $x \neq 0$ , divide by  $x^3$  getting

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0. \text{ This is a reciprocal equation.}$$

Plan. To solve it, rewrite it, adding 1 to each side.

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} + 1 = 1 + 1$$

$$\text{Let } x + \frac{1}{x} = z$$

$$x^2 + \frac{1}{x^2} = z^2 - 2$$

Substitute, get  $z^2 + z - 1 = 0$

$$z = \frac{-1 \pm \sqrt{5}}{2}$$

$$x + \frac{1}{x} = \frac{-1 + \sqrt{5}}{2} \quad x + \frac{1}{x} = \frac{-1 - \sqrt{5}}{2}$$

$$x^2 - \frac{-1 + \sqrt{5}}{2}x + 1 = 0 \quad x^2 - \frac{-1 - \sqrt{5}}{2}x + 1 = 0$$

$$x = \frac{\frac{-1 + \sqrt{5}}{2} \pm \sqrt{\left(\frac{-1 + \sqrt{5}}{2}\right)^2 - 4}}{2} \quad x = \frac{\frac{-1 - \sqrt{5}}{2} \pm \sqrt{\left(\frac{-1 - \sqrt{5}}{2}\right)^2 - 4}}{2}$$

$$x = \frac{\frac{-1 + \sqrt{5}}{2} \pm \frac{1}{2}\sqrt{10 - 2\sqrt{5}}}{2} \quad x = \frac{\frac{-1 - \sqrt{5}}{2} \pm \frac{1}{2}\sqrt{10 + 2\sqrt{5}}}{2}$$

$$x = \frac{-1 + \sqrt{5}}{4} \pm \frac{1}{4}\sqrt{10 + 2\sqrt{5}} \quad x = \frac{-1 - \sqrt{5}}{4} \pm \frac{1}{4}\sqrt{10 - 2\sqrt{5}}$$

The four roots are therefore:

$$x_1 = \frac{-1 + \sqrt{5}}{4} + \frac{1}{4}\sqrt{10 + 2\sqrt{5}}$$

$$x_2 = \frac{-1 + \sqrt{5}}{4} - \frac{1}{4}\sqrt{10 + 2\sqrt{5}}$$

1010

$$\alpha_2 = -\frac{1}{4} - \frac{\sqrt{5}}{4} + \frac{1}{4} i \sqrt{10 - 2\sqrt{5}}$$

$$\alpha_3 = -\frac{1}{4} - \frac{\sqrt{5}}{4} - \frac{1}{4} i \sqrt{10 - 2\sqrt{5}}$$

It would seem, therefore, that to get the Galois Domain for our equation it would be necessary to adjoin all our roots,  $R(1, \alpha, \alpha_1, \alpha_2, \alpha_3)$ . But we note that by adjoining  $\sqrt{5+\sqrt{5}}$  we get a domain that includes  $\sqrt{5}$ , because by multiplication by itself  $\sqrt{5+\sqrt{5}}$  will introduce  $\sqrt{5}$  in the domain. Also, by adjoining the  $\sqrt{2}$ , by multiplication  $\sqrt{2} \cdot \sqrt{5+\sqrt{5}}$  gives  $\sqrt{10+2\sqrt{5}}$ . Our  $\sqrt{-1} = i$ , of course, must be adjoined. Therefore, the adjoining of  $\sqrt{2}$ ,  $\sqrt{5+\sqrt{5}}$ , i will give  $R(1, \alpha)$  and also  $R(1, \alpha_1)$  thus  $R(1, \alpha) = R(1, \alpha_1)$ . Similarly the adjoining of  $\sqrt{2}$ ,  $\sqrt{5-\sqrt{5}}$ , i will give  $R(1, \alpha_2)$  and also  $R(1, \alpha_3)$ , and thus  $R(1, \alpha_2) = R(1, \alpha_3)$ .

Furthermore, if we can show that either  $\alpha$  or  $\alpha_1$  can be obtained from either  $\alpha_2$  or  $\alpha_3$  by the use only of the four fundamental operations, then we will have shown that  $R(1, \alpha) = R(1, \alpha_1) = R(1, \alpha_2) = R(1, \alpha_3)$  and it will not be necessary to adjoin to the new domain both  $\sqrt{5+\sqrt{5}}$  and  $\sqrt{5-\sqrt{5}}$ . We do this by proving  $\alpha = \alpha_3^2$

$$\alpha_3 = -\frac{1}{4} - \frac{\sqrt{5}}{4} - \frac{1}{4} i \sqrt{10 - 2\sqrt{5}} = -\frac{1}{4} [1 + \sqrt{5} + i \sqrt{10 - 2\sqrt{5}}]$$

$$\alpha_3^2 = \frac{1}{16} [1 + 2\sqrt{5} + 5 - 10 + 2\sqrt{5} + 2(1 + \sqrt{5}) i \sqrt{10 - 2\sqrt{5}}]$$

$$= \frac{1}{16} [-4 + 4\sqrt{5} + 2i(1 + \sqrt{5})\sqrt{10 - 2\sqrt{5}}]$$

$$= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i(1 + \sqrt{5})}{8} \sqrt{10 - 2\sqrt{5}}$$

$$a_2 = -\frac{1}{4} - \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{10 - 2\sqrt{5}}$$

$$a_3 = -\frac{1}{4} - \frac{\sqrt{5}}{4} - \frac{1}{4} \sqrt{10 - 2\sqrt{5}}$$

It would seem, therefore, that to get the Galois Domain for our equation it would be necessary to adjoin all our roots,  $R(1, a_1, a_2, a_3)$ . But we note that by adjoining  $\sqrt{5}$  we get a domain that includes  $\sqrt{5}$ , because by multiplication by  $\sqrt{5}$  itself  $\sqrt{5} \cdot \sqrt{5}$  will introduce  $\sqrt{5}$  in the domain. Also, by adjoining the  $\sqrt{5}$ , by multiplication  $\sqrt{5} \cdot \sqrt{5} \cdot \sqrt{5}$  gives  $\sqrt{5} \cdot \sqrt{5} \cdot \sqrt{5} = 5$ . Our  $\sqrt{5} = 1$  of course, must be adjoined. Therefore, the adjoining of  $\sqrt{5}$ ,  $\sqrt{5} \cdot \sqrt{5}$ , 1 will give  $R(1, a_1)$  and also  $R(1, a_2)$  since  $R(1, a_1) = R(1, a_2)$ . Similarly the adjoining of  $\sqrt{5}$ ,  $\sqrt{5} \cdot \sqrt{5}$ , 1 will give  $R(1, a_3)$  and also  $R(1, a_1)$ , and thus  $R(1, a_3) = R(1, a_1)$ .

Furthermore, if we can show that either  $a_1$  or  $a_2$  can be obtained from either  $a_3$  or  $a_4$  by the use only of the four fundamental operations, then we will have shown that  $R(1, a_1) = R(1, a_2) = R(1, a_3) = R(1, a_4)$  and it will not be necessary to adjoin to the new domain both  $\sqrt{5} \cdot \sqrt{5}$  and  $\sqrt{5} \cdot \sqrt{5}$ . We do this by

$$\text{proving } a_1 = a_3$$

$$a_1 = -\frac{1}{4} - \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{10 - 2\sqrt{5}} = -\frac{1}{4} - \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{10 - 2\sqrt{5}}$$

$$a_3 = -\frac{1}{4} - \frac{\sqrt{5}}{4} - \frac{1}{4} \sqrt{10 - 2\sqrt{5}} = -\frac{1}{4} - \frac{\sqrt{5}}{4} - \frac{1}{4} \sqrt{10 - 2\sqrt{5}}$$

$$a_1 - a_3 = \frac{1}{2} \sqrt{10 - 2\sqrt{5}} = \frac{1}{2} \sqrt{10 - 2\sqrt{5}}$$

$$a_1 + a_3 = -\frac{1}{2} - \frac{\sqrt{5}}{2} = -\frac{1}{2} - \frac{\sqrt{5}}{2}$$

$$(a_1 - a_3)^2 = \frac{1}{4} (10 - 2\sqrt{5}) = \frac{5}{2} - \frac{\sqrt{5}}{2}$$

$$(a_1 + a_3)^2 = \frac{1}{4} (1 + 2\sqrt{5} + 5) = \frac{3}{2} + \frac{\sqrt{5}}{2}$$

$$(a_1 - a_3)^2 + (a_1 + a_3)^2 = \frac{5}{2} - \frac{\sqrt{5}}{2} + \frac{3}{2} + \frac{\sqrt{5}}{2} = 4$$

$$(a_1 - a_3)^2 + (a_1 + a_3)^2 = 4$$

$$\begin{aligned}
 &= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i}{4} \left( \frac{1 + \sqrt{5}}{2} \right) \sqrt{10 - 2\sqrt{5}} \\
 &= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i}{4} \sqrt{\left( \frac{1 + \sqrt{5}}{2} \right)^2 (10 - 2\sqrt{5})} \\
 &= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i}{4} \sqrt{\left( \frac{6 + 2\sqrt{5}}{4} \right) (10 - 2\sqrt{5})} \\
 &= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i}{4} \sqrt{(3 + \sqrt{5})(5 - \sqrt{5})} \\
 &= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{i}{4} \sqrt{10 + 2\sqrt{5}}
 \end{aligned}$$

which is exactly  $\alpha$ .

Therefore  $\alpha = \alpha^2_3$  and so by adjoining the elements of  $\alpha$  only to  $R(1)$  and getting  $R(1, \alpha)$  we obtain all the elements that are found in  $R(1, \alpha_1)$ , or in  $R(1, \alpha_2)$ , or in  $R(1, \alpha_3)$ . Also, we noticed that to get  $R(1, \alpha)$ , we need only adjoin to  $R(1)$  the following:  $\sqrt{2}$ ,  $\sqrt{5+\sqrt{5}}$ ,  $i$ .

Therefore, the Galois Domain for our  $f(x) = x^4 + x^3 + x^2 + x + 1 = 0$  is  $R(1, \sqrt{2}, \sqrt{5+\sqrt{5}}, i)$ , and  $R(1, \alpha, \alpha_1, \alpha_2, \alpha_3) \equiv R(1, \alpha) \equiv R(1, \alpha_1) \equiv R(1, \alpha_2) \equiv R(1, \alpha_3)$ .

This Galois Domain which we have found is also a Normal Domain, because the conjugate domains  $R(1, \alpha)$ ,  $R(1, \alpha_1)$ ,  $R(1, \alpha_2)$ ,  $R(1, \alpha_3)$  are all identical. This is not a coincidence. As stated earlier, Galois' great achievements come in the reduction of any given domain to a normal domain, and the work in normal domains is much simpler than in the others.

#### CONCLUSION.

This concludes our introduction to the work of Galois.

$$\begin{aligned}
&= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} \left( \frac{1+\sqrt{5}}{2} \right) \sqrt{10-2\sqrt{5}} \\
&= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{\left( \frac{1+\sqrt{5}}{2} \right)^2 (10-2\sqrt{5})} \\
&= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{\frac{(8+2\sqrt{5})(10-2\sqrt{5})}{4}} \\
&= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{(8+\sqrt{5})(5-\sqrt{5})} \\
&= -\frac{1}{4} + \frac{\sqrt{5}}{4} + \frac{1}{4} \sqrt{10+2\sqrt{5}}
\end{aligned}$$

which is exactly  $\alpha$ .

Therefore  $\alpha = \alpha^2$  and so by adjoining the elements of  $\mathbb{Q}(\alpha)$  only to  $\mathbb{Q}$  and getting  $\mathbb{Q}(\alpha)$  we obtain all the elements that are found in  $\mathbb{Q}(\alpha)$ , or in  $\mathbb{Q}(\alpha)$ . Also, we noticed that to get  $\mathbb{Q}(\alpha)$ , we need only adjoin to  $\mathbb{Q}$  the following:  $\sqrt{5}, \sqrt{5+\sqrt{5}}, i$ .

Therefore, the Galois domain for our  $\mathbb{Q}(x) = x^4 + x^3 + x^2 + x + 1 = 0$  is  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i)$ , and  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i) \cong \mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i) \cong \mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i)$ . This Galois domain which we have found is also a normal domain, because the conjugate domains  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i)$ ,  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, -i)$ ,  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, i)$ ,  $\mathbb{Q}(\sqrt{5}, \sqrt{5+\sqrt{5}}, -i)$  are all identical. This is not a coincidence. As stated earlier, Galois' great achievement came in the relation of any given domain to a normal domain, and the work in normal domains is much simpler than in the others.

### CONCLUSION

This concludes our introduction to the work of Galois.

To go much further will require the study first of substitutions and groups, both isomorphic and cyclic. A Galois resolvent is obtained. It is shown that an equation is reducible or irreducible according as its Galois group is intransitive or transitive. Incidentally, the constructions by ruler and compass can be introduced under cyclic equations. Gauss showed that when  $n$  is a prime of the form  $2^k + 1$ , the division of the circle into  $n$  equal parts by ruler and compasses is always possible. An equation is solvable (called metacyclic) when its solution can be reduced to a solution of a series of cyclic equations. From this a necessary and sufficient condition for the solvability of an algebraic equation of any degree is developed. In general, the equations of the 5th degree and higher do not conform to the requirements of the conditions and so are not solvable by the use of radicals. However, there are many equations of the 5th or higher degree which may be of special form and so may reduce to a solvable case.

To go much further will require the study first of substitution  
and groups, both isomorphism and cyclic. A Galois resolvent is  
obtained. It is shown that an equation is reducible or irredu-  
cible according as the Galois group is transitive or intransi-  
tive. Incidentally, the construction by ruler and compass can  
be introduced under cyclic equations. Gauss showed that when  $n$   
is a prime of the form  $2^k + 1$ , the division of the circle into  $n$   
equal parts by ruler and compass is always possible. An equa-  
tion is solvable (called metacyclic) when its solution can be  
reduced to a solution of a series of cyclic equations. From  
this a necessary and sufficient condition for the solvability  
of an algebraic equation of any degree is developed. In gen-  
eral, the equations of the 5th degree and higher do not conform  
to the requirements of the conditions and so are not solvable  
by the use of radicals. However, there are many equations of  
the 5th or higher degree which may be of special form and so  
may reduce to a solvable case.

BIBLIOGRAPHY

- S. M. Barton: An Elementary Treatise on the Theory of Equations.  
Published by D. C. Heath and Company, 1903.  
Relation between roots and coefficients and symmetric functions.
- Oskar Bolza: On the Theory of Substitution - Groups and its Application to Algebraic Equations.  
Published in American Journal of Mathematics, Volume XIII, 1891.  
1st part on fundamental propositions in substitution groups  
2nd part on Galois Theory based on Jordan's "Traité des Substitutions", Serret's "Cours d'algèbre supérieure", and Netto's "Substitution-Theorie".  
This is a very clear exposition.
- Oskar Bolza: Review of Netto's Theory of Substitution.  
Translated by F. N. Cole.  
Published in Bulletin of the American (New York) Mathematical Society, Volume II, October 1892-July 1893.
- W. S. Burnside and A. W. Panton:  
The Theory of Equations, Volume II.  
Published by Longmans, Green and Company, 1901.  
Excellent on substitution groups. Galois resolvent and algebraic solution of equations.
- Florian Cajori: A History of Mathematics.  
Published by The MacMillan Company, 1929.  
History of algebra in terms of the great men who advanced it.
- Florian Cajori: An Introduction to the Modern Theory of Equations.  
Published by the MacMillan Company, 1930.  
The general presentation of material in this paper followed the logical presentation from this book.
- L. E. Dickson: Modern Algebraic Theories.  
Published by B. H. Sanborn and Company, 1926.  
The complete Galois Theory, but not in detail.

# BIBLIOGRAPHY

- E. W. Barton: An Elementary Treatise on the Theory of Equations.  
Published by D. C. Heath and Company, 1908.  
Relation between roots and coefficients and symmetric functions.
- Oskar Polka: On the Theory of Substitution - Groups and its Application to Algebraic Equations.  
Published in American Journal of Mathematics, Volume XIII, 1891.  
1st part on fundamental propositions in substitution groups.  
2nd part on Galois Theory based on Jordan's "Traité des Substitutions", Serret's "Cours d'algèbre supérieure", and Netto's "Substitutionentheorie".  
This is a very clear exposition.
- Oskar Polka: Review of Netto's Theory of Substitution.  
Translated by A. W. Gale.  
Published in Bulletin of the American Mathematical Society, Volume II, October 1892, July 1893.
- W. S. Burnside and A. W. Panton: The Theory of Equations, Volume II.  
Published by Longmans, Green and Company, 1901.  
Excellent on substitution groups. Galois, resolvent and algebraic solution of equations.
- Florian Cajori: A History of Mathematics.  
Published by The MacMillan Company, 1899.  
History of algebra in terms of the great men who advanced it.
- Florian Cajori: An Introduction to the Modern Theory of Equations.  
Published by The MacMillan Company, 1900.  
The general presentation of material in this paper followed the logical presentation from this book.
- L. E. Dickson: Modern Algebraic Theories.  
Published by B. F. Shober and Company, 1926.  
The complete Galois Theory, but not in detail.

- L. E. Dickson: Introduction to the Theory of Algebraic Equations.  
Published by John Wiley and Sons, 1903.  
Here is contained the complete theories of Lagrange, Cauchy, Abel, and Galois. An advanced book.
- Harris Hancock: Foundations of the Theory of Algebraic Numbers, Volume I.  
Published by the MacMillan Company, 1931.  
On realms or domains and the rational domain.
- M. Camille Jordan: Traité des Substitutions et des Équations Algébriques.  
Published by Gauthier-Villars, Paris, 1870.  
On group theory and substitutions.
- G. B. Mathews: Algebraic Equations.  
Published by the Cambridge University Press, 1915. No. 6 in Cambridge Tracts in Mathematics and Physics.  
Material for further completion of study.
- G. A. Miller, H. F. Blichfeldt, L. E. Dickson: Theory and Application of Finite Groups.  
Published by John Wiley and Sons, 1916.  
Complete group theory.
- Eugen Netto: The Theory of Substitutions and its Application to Algebra.  
Translated by F. N. Cole.  
Published by The Inland Press, Ann Arbor, Michigan, 1892.  
A complete but difficult and complicated presentation.
- Emile Picard: Traité d'analyse, Volume 3.  
Published by Gauthier-Villars et Fils, Paris, 1896.  
The fundamental theorem of Galois and the group of an algebraic equation with substitutions.
- James Pierpont: Galois Theory of Algebraic Equations in Annals of Mathematics.  
1st part, explanation of theory in Volume I, 2nd series, 1899-1900.  
Published by Salem Press Company, Salem, Massachusetts, under auspices of Harvard University.

I. E. Dickson: Introduction to the Theory of Algebraic Equations.  
Published by John Wiley and Sons, 1908.  
Here is contained the complete theories of  
Lagrange, Cauchy, Abel, and Galois. An ad-  
vanced book.

Henri Poincaré: Foundations of the Theory of Algebraic Numbers.  
Volume I.  
Published by the MacMillan Company, 1921.  
On residues on domains and the rational domain.

M. Camille Jordan: Traité des Substitutions et des Équations  
Algébriques.  
Published by Gauthier-Villars, Paris, 1870.  
On group theory and substitutions.

G. E. Matthews: Algebraic Equations.  
Published by the Cambridge University Press,  
1917. No. 6 in Cambridge Tracts in Mathematics  
and Physics.  
Material for further completion of study.

C. A. Miller, H. F. Blichfeldt, I. E. Dickson:  
Theory and Application of Finite Groups.  
Published by John Wiley and Sons, 1916.  
Complete group theory.

Eugen Netto: The Theory of Substitutions and its Application  
to Algebra.  
Translated by F. A. Cole.  
Published by The Indiana Press, Ann Arbor,  
Michigan, 1927.  
A complete but difficult and complicated pres-  
entation.

Paul F. Smith: Traité d'analyse, Volume 3.  
Published by Gauthier-Villars et Fils, Paris,  
1898.  
The fundamental theories of Galois and the group  
of an algebraic equation with substitutions.

James Pierpont: Galois Theory of Algebraic Equations.  
In Annals of Mathematics.  
1st part, explanation of theory in Volume I,  
2nd series, 1899-1900.  
Published by John Press Company, Salem,  
Massachusetts, under auspices of Harvard  
University.

2nd part, application of theory in Volume II,  
2nd series, 1900-1901.

Published by Longmans, Green and Company.  
An excellent discussion based on lectures at  
American Mathematical Society at Buffalo,  
September 1896.

James Pierpont: Life and History of Galois.  
Published in Bulletin of American Mathematical  
Society, Series 2, Volume 4, 1897-1899.  
Galois' life was taken from this article.

L. W. Reid: The Elements of the Theory of Algebraic Numbers.  
Published by The MacMillan Company, 1910.  
Information on domains.

Joseph Alfred Serret: Cours d'Algèbre Supérieure, Volume 2.  
Published by Gauthier-Villars, Paris, 1879.  
Chapter V on the discoveries of Galois and the  
application to irreducible equations.

David Eugene Smith: A Source Book in Mathematics.  
Published by the McGraw Hill Book Company,  
1929.  
Translation of letter from Galois to  
M. Chevalier.

Heinrich Weber: Lehrbuch der Algebra, Volume 1.  
Published by Braunschweig, 1898.  
Complete development of Galois Theory.

2nd part, application of theory in Volume II,  
2nd series, 1900-1901.  
Published by Hermann, Green and Company.  
An excellent discussion based on lectures at  
American Mathematical Society in Berlin,  
September 1896.

James E. Littlewood: *Algebra and History of Galois.*  
Published in Bulletin of American Mathematical  
Society, Series 2, Volume 4, 1897-1898.  
Galois' life was taken from this article.

L. W. Reid: *The Elements of the Theory of Algebraic Numbers.*  
Published by The Macmillan Company, 1910.  
Information on domains.

Joseph Alfred Serret: *Cours d'Algebre Supérieure, Volume 2.*  
Published by Gauthier-Villars, Paris, 1879.  
Chapter 7 on the divisors of Galois and the  
application to irreducible equations.

David Eugene Smith: *A Source Book in Mathematics.*  
Published by the McGraw Hill Book Company,  
1925.  
Translation of letter from Galois to  
M. Chevalier.

Heinrich Weber: *Lehrbuch der Algebra, Volume I.*  
Published by Braunschweig, 1898.  
Complete development of Galois theory.





BOSTON UNIVERSITY



1 1719 02552 8607

